#4

Attorney Docket No.:04329.2319

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	:	
Tooru KAMIBAYASHI et al.	:	
Serial No.: 09/593,864	:	Group Art Unit: 2766
Filed: June 15, 2000	:	Examiner: Not Assigned

For: MUTUAL AUTHENTICATION METHOD, RECORDING APPARATUS, REPRODUCING APPARATUS, AND RECORDING MEDIUM

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Under the provisions of 35 U.S.C. § 119, Applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 11-170187, filed June 16, 1999, for the above-identified U.S. patent application.

In support of Applicants' claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

By: Richard V. Burgujian 20,338 /a
Richard V. Burgujian
Reg. No. 31,744

Date: November 3, 2000
RVB/FPD/dvz
Enclosure

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　６月１６日

出 願 番 号
Application Number: 平成１１年特許願第１７０１８７号

出 願 人
Applicant (s): 株式会社東芝
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　６月２３日

特 許 庁 長 官
Commissioner,
Patent Office

近 藤 隆 彦

出証番号　出証特２０００－３０４６６７５

【書類名】　特許願

【整理番号】　A009903625

【提出日】　平成11年 6月16日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F　7/00

【発明の名称】　相互認証方法および記録装置および再生装置および記録媒体

【請求項の数】　8

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　上林　達

【発明者】

【住所又は居所】　東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

【氏名】　山田　尚志

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内

【氏名】　岩崎　博

【発明者】

【住所又は居所】　東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

【氏名】　田村　正文

【発明者】

【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

【氏名】　石橋　泰博

出証特２０００－３０４６６７５

【発明者】
【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内
【氏名】　加藤　拓
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　館林　誠
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　原田　俊治
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　相互認証方法および記録装置および再生装置および記録媒体

【特許請求の範囲】

【請求項１】　演算処理機能を有する記録媒体に複製コンテンツを記録する記録装置と該記録媒体との間の相互認証方法において、

前記記録媒体は、少なくとも該記録媒体に依存する第１の情報と、前記記録装置と相互認証を行う際に該記録装置と共有すべき該記録媒体に依存する第２の情報とを記憶し、

前記記録装置は、前記記録媒体から得られた前記第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第２の情報とを用いて前記記録装置と前記記録媒体との間で相互認証を行うことを特徴とする相互認証方法。

【請求項２】　演算処理機能を有する記録媒体に記録された複製コンテンツを再生する再生装置と該記録媒体との間の相互認証方法において、

前記記録媒体は、少なくとも該記録媒体に依存する第１の情報と、前記再生装置と相互認証を行う際に該再生装置と共有すべき該記録媒体に依存する第２の情報とを記憶し、

前記再生装置は、前記記録媒体から得られた前記第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第２の情報とを用いて前記再生装置と前記記録媒体との間で相互認証を行うことを特徴とする相互認証方法。

【請求項３】　前記記録媒体から得られた暗号鍵で前記第１の情報を暗号化して前記認証情報を生成することを特徴とする請求項１または２記載の相互認証方法。

【請求項４】　記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に複製コンテンツを記録する記録装置において、

前記記録媒体から得られた該記録媒体に依存する第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成す

る生成手段と、

この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、

を具備したことを特徴とする記録装置。

【請求項５】　前記記録媒体から得られた暗号鍵で前記第１の情報を暗号化して前記認証情報を生成することを特徴とする請求項４記載の記録装置。

【請求項６】　記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に記録された複製コンテンツを再生する再生装置において、

前記記録媒体から得られた該記録媒体に依存する第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成する生成手段と、

この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、

を具備したことを特徴とする再生装置。

【請求項７】　前記記録媒体から得られた暗号鍵で前記第１の情報を暗号化して前記認証情報を生成することを特徴とする請求項６記載の再生装置。

【請求項８】　演算処理機能を有する記録媒体であって、

自己に固有の第１の情報と、記録媒体に複製コンテンツを記録する記録装置および複製コンテンツを再生する再生装置との間で相互認証を行う際に該記録装置および該再生装置と共有すべき該記録媒体に依存する第２の情報とを予め記憶した記憶手段と、

前記記録装置および再生装置にて前記第１の情報に基づき生成された認証情報と、前記第２の情報とを用いて自己と前記記録装置および自己と前記再生装置との間で相互認証を行う相互認証手段と、

を具備したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えば、複製コンテンツの数を規制して著作権の保護を図るコンテ

ンツ管理方法を用いた記録装置、再生装置、記録媒体の間の相互認証方法およびそれを用いた記録装置、再生装置、記録媒体に関する。

【０００２】

【従来の技術】

従来、コンテンツ（著作物等）は、コピー管理が行われてきた。コピー世代管理やコピーの数を管理する事により、著作権保護と利用の便宜のバランスをとってきた。

【０００３】

さらに、コピー管理に代わって、「移動」の概念が登場してきた。コピーがオリジナルのデータを消去しないのと対照的に、移動は、異なった場所（記録媒体（メディア））にデータを転送すると共に、オリジナルデータを消去する。コンテンツのデジタル化とネットワーク等の普及が、移動によるコピープロテクションが登場した背景にある。

【０００４】

【発明が解決しようとする課題】

近年、ネットワーク等を通じたオリジナルに忠実なコピーが可能になったため、コピー管理だけでは、著作権保護が困難になってきた。また、メディアからメディアへの無制限な移動、例えば、データの営利目的の（移動による）配布は、著作権管理を行うことができない。

【０００５】

このように、オリジナルのデータ（特に、著作権保護の対象となるようなコンテンツ）の複製を確実に管理することが困難となってきた。

【０００６】

そこで、本発明は、低コストの記録媒体を用いて、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間の高い情報セキュリティ性を実現することが可能な相互認証方法および、それを用いたコンテンツの記録装置、再生装置、記録媒体を提供することを目的とする。本発明は、特に、複製コンテンツの数を規制して著作権の保護を図るコンテンツ管理に有効である。

【０００７】

【課題を解決するための手段】

（１）本発明の相互認証方法は、演算処理機能を有する記録媒体に複製コンテンツを記録する記録装置（演算処理機能を有する記録媒体に記録された複製コンテンツを再生する再生装置）と該記録媒体との間の相互認証方法において、前記記録媒体は、少なくとも該記録媒体に依存する第１の情報と、前記記録装置（再生装置）と相互認証を行う際に該記録装置（再生装置）と共有すべき該記録媒体に依存する第２の情報とを記憶し、前記記録装置（再生装置）は、前記記録媒体から得られた前記第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第２の情報とを用いて前記記録装置（再生装置）と前記記録媒体との間で相互認証を行うことを特徴とする。

【０００８】

本発明によれば、記録媒体にグローバルシークレットな情報（全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報）を記録する必要がないので、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【０００９】

（２）本発明の記録装置は、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に複製コンテンツを記録する記録装置において、

前記記録媒体から得られた該記録媒体に依存する第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成する生成手段と、

この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、

を具備する。

【００１０】

本発明によれば、記録媒体にグローバルシークレットな情報（全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報）を記録する必要がないので、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【００１１】

（３）本発明の再生装置は、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に記録された複製コンテンツを再生する再生装置において、

前記記録媒体から得られた該記録媒体に依存する第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成する生成手段と、

この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、

を具備する。

【００１２】

本発明によれば、記録媒体にグローバルシークレットな情報（全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報）を記録する必要がないので、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【００１３】

（４）本発明の記録媒体は、演算処理機能を有する記録媒体であって、

自己に固有の第１の情報と、記録媒体に複製コンテンツを記録する記録装置および複製コンテンツを再生する再生装置との間で相互認証を行う際に該記録装置および該再生装置と共有すべき該記録媒体に依存する第２の情報とを予め記憶した記憶手段と、

前記記録装置および再生装置にて前記第１の情報に基づき生成された認証情報と、前記第２の情報とを用いて自己と前記記録装置および自己と前記再生装置との間で相互認証を行う相互認証手段と、

を具備する。

【００１４】

本発明によれば、記録媒体にグローバルシークレットな情報（全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報）を記録する必要がないので、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【００１５】

【発明の実施の形態】

以下、本発明の一実施形態について図面を参照して説明する。

【００１６】

図１は、本実施形態にかかる記録媒体（メディア）に記憶できる複製コンテンツの数を規制し、メディアへの複製コンテンツの記録、メディアに記録された複製コンテンツの再生等を行う音楽コンテンツ利用管理システム（以下、簡単にＬＣＭと呼ぶことがある）１の構成例を示したものである。なお、ここでは、コンテンツとして音楽を一例として用いているが、この場合に限らす、映画や、ゲームソフト等であってもよい。また、メディアとしてメモリカード（ＭＣ）を用いているが、この場合に限るものではなく、フロッピーディスク、ＤＶＤ等の各種記録媒体であってもよい。

【００１７】

ＥＭＤ（Electronic Music Distributor）は、音楽配信サーバまたは音楽配信放送局である。

【００１８】

コンテンツ利用管理システム１は、例えば、パソコン（ＰＣ）であり、複数のＥＭＤ（ここでは、ＥＭＤ＃１～＃３）に対応した受信部＃１～＃３を具備しており、ＥＭＤが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツの復号鍵Ｋｃ）などを受信する。受信部＃１～＃３は、再生機能や課金機能を有していても良い。配信された音楽コンテンツを試聴する為に再生

機能が用いられる。又、課金機能を利用して、気に入ったコンテンツを購入する事が可能である。

【００１９】

ＬＣＭ１は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：ＳＭＳで、以下、簡単にＳＭＳと呼ぶことがある）２を具備し、利用者が購入したコンテンツはＥＭＤインタフェース（Ｉ／Ｆ）部３を経由してＳＭＳ２に蓄積される。音楽コンテンツは、必要に応じてＥＭＤＩ／Ｆ部３で復号され、形式変換や再暗号化が施される。ＳＭＳ２が暗号化コンテンツを受け取ると、それを音楽データ格納部１０に格納し、音楽データ復号鍵をライセンス格納部９に格納する。ＳＭＳ２が再生機能を有していても良い。当該再生機能により、ＳＭＳ２が管理する音楽コンテンツをＰＣ上で再生する事ができる。

【００２０】

ＳＭＳ２は、メディア（以下、簡単にＭＣ（memory card）と呼ぶことがある）１３に対してコンテンツデータを出力する機能を有している。ＭＣ１３を記録再生装置（以下、簡単にＰＤ（Portable Device）と呼ぶことがある）１２にセットし、ＭＣ１３に記録されたコンテンツを再生することができる。

【００２１】

ＳＭＳ２からＭＣ１３へのコンテンツの記録はメディア（ＭＣ）インタフェース（Ｉ／Ｆ）部６を通じて直接行われるか、又はＰＤ１２を経由して行うことができる。

【００２２】

デバイスＩＤ格納部４は、例えば、ＲＯＭで構成され、当該ＬＣＭの識別情報（デバイスＩＤ）が格納されている。

【００２３】

ＭＣ１３は、そのメディア固有かつ書き換え不能の識別情報（ＭＩＤ）を有しており、ＭＣ１３に格納されるコンテンツは、ＭＣ１３に依存する暗号化鍵で暗号化されていてもよい。

【００２４】

まず、チェックイン／チェックアウトについて、図１のＬＣＭ１に則して説明

する。

【００２５】

チェックアウトとは、ＬＭＳ１が「親」としてのコンテンツを格納しており、ＭＣ１３に、その複製を「子」コンテンツとしてコピーすることをいう。「子」コンテンツはＰＤ１２で自由に再生する事が可能であるが、「子」から「孫」コンテンツを作成する事は許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、ＭＣ１３をＬＣＭ１に接続し、ＬＣＭ１が「子」コンテンツを消去（又は利用不能）する事で、ＬＣＭ１内の「親」コンテンツは「子」を１つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【００２６】

このチェックイン／チェックアウトを単純に、従来からのＬＣＭ１で実現しようとすると、実際、次の様な「攻撃」が存在する。すなわち、ＭＣ１３に格納された「子」を別の記憶メディアに（ＭＩＤを除いて）退避しておき、ＭＣ１３の「子」を「親」にチェックインする。次いで、先に退避しておいた「子」を当該ＭＣ１３に書き戻す。既にチェックインは済んでいるので、ＬＣＭ１上の「親」は別のＭＣ１３に「子」をコピーして良い。この方法で、任意の個数だけ利用可能な「子」を作る事が可能である。

【００２７】

上述の「攻撃」には、ＭＣ１３とＬＣＭ１とのデータ転送の際に認証を行う事により、対抗可能である。すなわち、ＭＣ１３は正当なＬＣＭ１以外からのデータ転送を受け付けず、ＬＣＭ１が正当なＭＣ１３以外からのデータ転送を受け付けないと仮定する。この場合、ＭＣ１３内の「子」を別の記録メディアに退避する事はできない。又、ＬＣＭ１に対して、偽って、チェックインすることもできない。従って、上述の「攻撃」は破綻する。

【００２８】

ところが、実は、ＬＣＭ１とＭＣ１３との認証を前提としても、チェックイン／チェックアウトは実現できない。次の様な「攻撃」が存在するからである。すなわち、まず、ＬＣＭ１上の「親」が「子」を作っていない状態で、ＬＣＭ１の

データ（特に、ライセンス格納部９の情報）を別の記憶メディアにバックアップする。ＭＣ１３に「子」をコピーした後、バックアップしたＬＣＭ１のデータを復帰する。ＬＣＭ１の「親」は「子」を作る前の状態に戻るから、別のＭＣ１３に「子」を作成する事ができる。この様にして、任意の数の「子」を作成する事が可能となってしまう。

【００２９】

そこで、このような攻撃にも対処できるチェックイン／チェックアウトを実現するために、ＭＣ１３内の記憶領域に、公開された手順では読み書きできない領域（秘匿領域）を設け、そこに相互認証に必要な情報やコンテンツ復号に必要な情報や、アクセス不可能であるデバイス（ＬＣＭ１、ＰＤ１２）の識別情報（デバイスＩＤ）のリスト（リボケーションリスト（ＲＶＣリスト））等を記録する（図２参照）。また、ＬＣＭ１の記憶領域（例えば、ＬＣＭ１がＰＣで構成されている場合には、ハードディスク（ＨＤＤ））上に非公開の手順でしかアクセスできない領域（秘匿領域）を設け、後述するような宿帳を当該秘匿領域に格納する（図２参照）。さらに、ＰＤ１２の記憶領域上にも非公開の手順でしかアクセスできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録するようにしてもよい（図２参照）。なお、ここでは、記憶領域中の秘匿領域以外の通常に手順にてアクセス可能な領域を公開領域と呼ぶ。

【００３０】

図１に示すように、ＬＣＭ１では、秘匿領域には、宿帳格納部８が設けられ、ＳＭＳ２にてこの宿帳格納部８にアクセスするための秘匿された特定の手続が行われた後、秘匿領域からデータを読み取るための秘匿領域ドライバ７を具備している。

【００３１】

図４（ｃ）に示すように、ＭＣ１３は、その識別情報ＭＩＤを格納するための外部からは書換不可能で、コピーも不可能なような構成になっている識別情報格納部（ＲＯＭ）１３ｂと、秘匿領域１３ｃと、公開領域（読み書き可能なＲＡＭ）１３ａと、秘匿領域１３ｃにアクセスされる度に認証部１３ｄにて認証を行って、正当な相手であると確認されたときに初めて秘匿領域１３ｃにアクセス可能

なようにゲートを開くスイッチ（ＳＷ）１３ｅを具備する。

【００３２】

なお、本実施形態で利用可能なＭＣ１３は、３種類あり、図４（ｃ）に示すような、識別情報ＭＩＤと秘匿領域とを両方兼ね備えているＭＣ１３の種別を「レベル２」と呼ぶ。秘匿領域は持たないが識別情報ＭＩＤは持つ図４（ｂ）に示すようなＭＣ１３の種別を「レベル１」と呼ぶ。秘匿領域も識別情報も持たない図４（ａ）に示すような公開領域だけのＭＣ１３の種別を「レベル０」と呼ぶことにする。これら種別は、例えば、識別情報ＭＩＤの有無でレベル０とそれ以外の種別とが判別でき、さらに、識別情報ＭＩＤの構成からレベル１とレベル２とを判別する。例えば、識別情報が連続した数値であるとき、所定値以上はレベル２であるとする。

【００３３】

以下、特に断らない限り、レベル２のＭＣ１３の場合を例にとり説明する。

【００３４】

このＭＣ１３は、ＬＣＭ１に接続されたＰＤ１２にセットして用いる場合とＬＣＭ１に直接セットして用いる場合とがある。

【００３５】

図３は、ＰＤ１２の構成例を示したもので、ＭＣ１３は、メディアインタフェース（Ｉ／Ｆ部）１２ｆにセットされる。ＬＣＭ１がＰＤ１２を介してＭＣ１３に読み書きする場合は、ＰＤ１２内の秘匿領域アクセス部を経由してＭＣ１３の秘匿領域にアクセスする。メディアＩ／Ｆ部１２ｆには、ＭＣ１３の秘匿領域にアクセスするための秘匿領域アクセス部を具備している。ＰＤ１２内の秘匿領域は、フラッシュメモリ１２ｄに設けられていても良い。ＲＯＭ１２ｃには、ＭＣ１３、ＬＣＭ１との間で相互認証を行うためのプログラムや、秘匿領域へアクセスするための認証手続を記述したプログラムや、ＭＣ１３の種別を判別するためのプログラムも書き込まれていて、このプログラムに従って、ＣＰＵ１２ａの制御の下、ＭＣ１３との間の各種認証、種別判別等の処理を実行するようになっている。

【００３６】

ＲＯＭ１２ｃには、ＰＤ１２の識別情報（デバイスＩＤ）が格納されていてもよい。また、例えば、フラッシュメモリ１２ｄに設けられた秘匿領域に秘匿デバイスＩＤ（ＳＰＤＩＤ）が予め格納されている。

【００３７】

図５は、ＬＣＭ１のメディアＩ／Ｆ部６の構成を示したもので、ＭＣ１３との間で相互認証を行うための認証部６ｃと、ＭＣ１３の種別を判別するメディア判別部６ｂと、これら全体を制御するための制御部６ａとから構成されている。認証部６ｃは、ＭＣ１３の秘匿領域にアクセスするための秘匿領域アクセス部でもある。

【００３８】

次に、ＬＣＭ１の秘匿領域に格納される宿帳について説明する。

【００３９】

ＳＭＳ２にて保持する全ての音楽コンテンツは、そのそれぞれを識別するための識別情報であるコンテンツＩＤ（ＴＩＤ）と、予め定められた複製可能コンテンツ数、すなわち、子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼ぶ。宿帳は、秘匿領域に設けられた宿帳格納部８に図７（ａ）に示すような形態で記録されている。

【００４０】

図７（ａ）において、例えば、コンテンツＩＤ「ＴＩＤ１」なる子の残数は「２」で、そのチェックアウトリストはＬ１である。

【００４１】

チェクアウトリストは、複製コンテンツ（子）を記録したＭＣ１３の識別情報のリストであって、例えば、図７（ａ）において、チェックアウトリストＬ１には「ｍ１」と「ｍ２」という識別情報を持つ２つのＭＣ１３にコンテンツＩＤ「ＴＩＤ１」なるコンテンツの子がチェックアウトされていることがわかる。

【００４２】

以下、次に示す項目の順に説明する。

【００４３】

（１）本発明の要旨である相互認証方法の概略

（２）レベル２のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

（３）レベル０のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

（１）本発明の要旨である相互認証方法の概略

前述したように、チェックイン／チェクアウトを安全に行うために、ＬＣＭ１、ＰＤ１２とＭＣ１３との間で（例えば、互いに同じアルゴリズムをもっているかの確認のための）相互認証を行う必要がある。一般に、相互認証処理には、相互認証を行う一方と他方とで共有する秘密の情報を持つ必要がある。従って、このような秘密情報を例えばＭＣ１３とＬＣＭ１およびＰＤ１２が持つことになる。情報セキュリティの観点から考えると、この秘密情報は、認証を行う度に毎回異なるものが生成されるといった動的なものであった方がよい。しかし、ＭＣ１３というメディア自体にそのような秘密情報を生成するための高度な機能を追加すると、メディアが高価になってしまう。メディアを広く一般大衆に普及させるためには、できるだけ安価である方が望ましい。従って、メディア（ＭＣ１３）のコスト低減化を考えれば、秘密情報をＭＣ１３に予め記憶させておく方がよい。

【００４４】

しかし、全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報（以下、このような情報をグローバルシークレットな情報と呼ぶ）を各メディアに予め記憶させた場合、ある１つのメディアからその秘密情報が何らかの方法により読まれてしまったとき、同じ秘密情報を記憶する他のメディアも不正に利用されてしまうという問題点があった。メディアにグローバルスシークレットな情報を持たせることは極めて危険である（図８（ａ）参照）。

【００４５】

ある１つのメディアに記憶されている秘密情報が不当に読まれてしまっても、不正に使用できるのは、その秘密情報が読まれしまったメディアだけであれば問題がないわけであるから、秘密情報は、個々のメディアに固有のものであればよ

い。

【００４６】

そこで、本発明は、個々のメディアにメディア毎にそれぞれ異なる相互認証のための秘密情報を記憶させておき、この情報を用いてＬＣＭ１あるいはＰＤ１２とＭＣ１３とが相互認証を行うことにより、低コストなメディアを用いた、よりセキュリティ性の高い安全な相互認証方法を提供することを目的とする。すなわち、本実施形態で説明する相互認証方法は、図８（ｂ）に示すように、個々のメディア（レベル２のメディア）に相互認証（ＡＫＥ）のために必要な各メディア毎にそれぞれ異なる秘密情報（ここでは、秘匿メディアＩＤ（ＳＭＩＤ）で、これは、メディアＩＤを何らかの方法で取得した鍵情報ＫＭで予め暗号化されたもの）を（秘匿領域に）予め記憶させておき、ＬＣＭ１、ＰＤ１２には、そのメディアの識別情報（ＭＩＤ）を転送する。ＬＣＭ１あるいはＰＤ１２側では、ＭＩＤと、先に何らかの方法で取得した情報（ＫＭ）とを用いて相互認証のための情報（メディアのもつＳＭＩＤと同じもの）を所定のアルゴリズムを用いて生成して認証処理（ＡＫＥ）を行う。

【００４７】

このように、ＭＣ１３にはそれぞれに固有の秘密情報（ＳＭＩＤ）を持たせておくだけで、ＬＣＭ１、ＰＤ１２がメディアから転送されてきた各メディア毎に固有の情報（ＭＩＤ）を基に秘密情報（ＳＭＩＤ）を生成することにより、メディアに負荷をかけずに安全な相互認証が行える。

【００４８】

なお、以下の説明において、本発明の要旨にかかる相互認証処理をＡＫＥと呼ぶことにする。

【００４９】

ＭＣ１３がＬＣＭ１のメディアＩ／Ｆ部６、あるいは、ＰＤ１２にセットされると、まず、メディアＩＦ部６とＭＣ１３との間、あるいは、ＰＤ１２とＭＣ１３との間で相互認証が行われてもよい（図９のステップＳ１）、そして、双方にて正当な（例えば、同じ規格のハードウエア構成である）相手であると判断されたとき（ステップＳ２）、メディアＩ／Ｆ部６あるいはＰＤ１２はＭＣ１３か

ら読み取った識別情報ＭＩＤを基に、ＭＣ１３の種別を判別する（ステップＳ３）。そして、メディアＩ／Ｆ部６あるいはＰＤ１２は、その種別に応じたチェックイン／チェックアウト／再生処理を実行する（ステップＳ６）。

【００５０】

なお、図９のステップＳ１における相互認証は、必ずしも図８（ｂ）に示したような本発明の要旨にかかる相互認証である必要はない。

【００５１】

また、ＭＣ１３にはレベル０からレベル２までの３種類があると説明したが、ここでは、レベル０とレベル２の２種類のＭＣ１３を対象として、図９以降の複製コンテンツのチェックイン／チェックアウト／再生処理動作について説明する。

【００５２】

さらに、以下の説明では、省略しているが、ＬＣＭ１とＭＣ１３との間、ＬＣＭ１とＰＤ１２との間、ＰＤ１２とＭＣ１３との間で、それぞれの秘匿領域にアクセスする際には、一方と他方との間で相互認証を行い、双方の正当性が確認されたらそれぞれの秘匿領域へのゲートを開き、秘匿領域へのアクセスが終了したら秘匿領域へのアクセスを可能にしていたゲートを閉じる仕組みになっているものとする。例えば、ＬＣＭ１とＭＣ１３との間において、ＳＭＳ２は、ＭＣ１３の秘匿領域１３ｃにアクセスすべく、ＭＣ１３との間で相互認証を行い、双方の正当性が確認されてスイッチ１３ｅにより秘匿領域１３ｃへのゲートが開かれると、秘匿領域１３ｃ内に鍵情報書込み、それが終了すると秘匿領域１３ｃへのアクセスを可能にしていたゲートがスイッチ１３ｅにより閉じられる仕組みになっている。

【００５３】

（２）　レベル２のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

図４（ｃ）に示したような構成のレベル２のＭＣ１３を用いたチェックイン／チェックアウト、再生処理動作について説明する。

【００５４】

チェックアウトの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介して（すなわち、ＭＣ１３をＬＣＭ１に接続されたＰＤ１２にセットして用いた場合）、ＳＭＳ２に対しなされた場合について、図１０を参照して説明する。

【００５５】

ＳＭＳ２は、宿帳のチェックアウト要求のあったコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の子の残数ｎを調べ、ｎ＞０のとき、デバイスＩＤ格納部４から当該ＬＣＭ１のデバイスＩＤ（ＬＣＭＩＤ）を読み出し、それをＭＣ１３へ転送する（ステップＳ１０１）。

【００５６】

ＭＣ１３では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ１０２）、登録されていないとき秘匿領域１３ｃにアクセスしてマスターキーＫＭを読み出して、ＬＣＭ１へ転送する（ステップＳ１０３）。ＭＣ１３は、さらに、識別情報格納部１３ｂから、その識別情報（ＭＩＤ）を読み出して同じくＬＣＭ１へ転送する（ステップＳ１０４）。

【００５７】

ＬＣＭ１では、ＭＣ１３から転送されてきたメディアＩＤ（ＭＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＭＩＤ］）を生成する（ステップＳ１０５）。

【００５８】

ＬＣＭ１では、この生成された情報ＫＭ［ＭＩＤ］を用いて相互認証処理（ＡＫＥ）を実行し、一方、ＭＣ１３でも秘匿メディアＩＤ（ＳＭＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（ステップＳ１０６）。この相互認証処理（ＡＫＥ）では、ＬＣＭ１とＭＣ１３とが同じ関数ｇ（ｘ、ｙ）、Ｈ（ｘ、ｙ）を共有していて、ＬＣＭ１で生成された情報ＫＭ［ＭＩＤ］が当該ＭＣ１３の秘匿メディアＩＤ（ＳＭＩＤ）と同じであるならば、相互認証処理（ＡＫＥ）により互いに一方が他方を正当であると確認できるようになっている。

【００５９】

ここで、図２１を参照して、ステップＳ１０６の相互認証処理（ＡＫＥ）の処理動作について説明する。

【００６０】

ＬＣＭ１は、乱数Ｒ１を発生し（ステップＳ３０１）して、それをＭＣ１３に転送するとともに、２つの変数ｘ、ｙを有する関数ｇ（ｘ、ｙ）の一方の変数に代入する。また、図１０のステップＳ１０５で生成された情報ＫＭ［ＭＩＤ］を関数ｇ（ｘ、ｙ）の他方の変数に代入して、関数ｇの値を求める（ステップＳ３０２）。

【００６１】

一方、ＭＣ１３でも、ＬＣＭ１から転送されてきた乱数Ｒ１を関数ｇ（ｘ、ｙ）の一方の変数に代入し、自身の秘匿メディアＩＤ（ＳＭＩＤ）を他方の変数に代入して、求めた関数ｇの値をＬＣＭ１へ転送する（ステップＳ３０３）。

【００６２】

ＬＣＭ１では、ＭＣ１３から転送されてきた関数ｇの値と、ＬＣＭ１側で求めた関数ｇの値とを比較し、一致していたら後続の処理を実行する。また、不一致であれば、この時点で、ＬＣＭ１側でのＡＫＥの処理を中止する（ステップＳ３０４）。

【００６３】

次に、ＭＣ１３では、乱数Ｒ２を発生し（ステップＳ３０５）して、それをＬＣＭ１に転送するとともに、２つの変数を有する関数ｇ（ｘ、ｙ）の一方の変数に代入する。また、当該ＭＣ１３の秘匿メディアＩＤ（ＳＭＩＤ）を関数ｇ（ｘ、ｙ）の他方の変数に代入して、関数ｇの値を求める（ステップＳ３０６）。

【００６４】

一方、ＬＣＭ１でも、ＭＣ１３から転送されてきた乱数Ｒ２を関数ｇ（ｘ、ｙ）の一方の変数に代入し、また、図１０のステップＳ１０５で生成された情報ＫＭ［ＭＩＤ］を関数ｇ（ｘ、ｙ）の他方の変数に代入して、関数ｇの値を求めたら、それをＭＣ１３へ転送する（ステップＳ３０７）。

【００６５】

ＭＣ１３では、ＬＣＭ１から転送されてきた関数ｇの値と、ＭＣ１３側で求め

た関数ｇの値とを比較し、一致していたら後続の処理を実行する。また、不一致であれば、この時点で、ＭＣ１３側でのＡＫＥの処理を中止する（ステップＳ３０８）。

【００６６】

ＭＣ１３では、ステップＳ３０８で、関数ｇの値が一致していたら、２つの変数を有する関数Ｈ（ｘ、ｙ）の一方の変数に乱数Ｒ２、他方の変数に当該ＭＣ１３の秘匿メディアＩＤ（ＳＭＩＤ）を代入して鍵情報ＫＴを生成する（ステップＳ３０９）。

【００６７】

一方、ＬＣＭ１でも、ステップＳ３０４で関数ｇの値が一致していたら、ＭＣ１３から転送されてきた乱数Ｒ２を関数Ｈ（ｘ、ｙ）の一方の変数に代入するとともに、図１０のステップＳ１０５で生成された情報ＫＭ［ＭＩＤ］を他方の変数に代入して鍵情報ＫＴを生成する（ステップＳ３１０）。

【００６８】

なお、ステップＳ３０４、ステップＳ３０８のそれぞれで関数ｇの値が一致したことによりＬＣＭ１とＭＣ１３のそれぞれで同じ関数Ｈ（ｘ、ｙ）を用いて生成される鍵情報ＫＴは同じものである。ＬＣＭ１とＭＣ１３のそれぞれでは、以降、この鍵情報ＫＴを用いてコンテンツ復号鍵Ｋｃの受け渡しを行うようになっている。

【００６９】

また、相互認証処理（ＡＫＥ）で生成される鍵情報ＫＴは、毎回異なるものである方が情報セキュリティ上望ましい。ここでは、鍵情報ＫＴを生成する関数Ｈに代入される２つの変数のうちの一方には、毎回新たに生成される乱数Ｒ２が代入されるので、毎回個となる鍵情報ＫＴが生成される。

【００７０】

図１０の説明に戻り、ステップＳ１０６において、ＬＣＭ１とＭＣ１３との間で相互に認証されたときは、ＭＣ１３では、生成した鍵情報ＫＴ（ここでは、ＫＴ１とする）を秘匿領域に格納する（ステップＳ１０７）。また、ＬＣＭ１では、暗号化コンテンツを復号するための復号鍵（コンテンツ復号鍵）Ｋｃをステッ

プＳ１０６で生成された鍵情報ＫＴ１で暗号化して（ＫＴ１［Ｋｃ］）ＭＣ１３へ転送し（ステップＳ１０８～ステップＳ１０９）、コンテンツ情報ＣをＫｃで暗号化して（Ｋｃ［Ｃ］）ＭＣ１３へ転送する（ステップＳ１１０～ステップＳ１１１）。

【００７１】

最後に、ＳＭＳ２は、図７（ｂ）に示すように、宿帳のチェックアウト要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎから「１」減算し、チェックアウトリストＬ１に、当該ＭＣ１３の識別情報「ｍ０」を追加する。

【００７２】

ＭＣ１３は、転送されてきた暗号化されたコンテンツ復号鍵ＫＴ１［Ｋｃ］、暗号化コンテンツＫｃ［Ｃ］を公開領域１３ａに格納する。

【００７３】

以上の処理が終了したときのＭＣ１３の記憶内容を図６に示す。

【００７４】

次に、再生の指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介してＳＭＳ２に、あるいは、ＰＤ１２に対しなされた場合について、図１１を参照して説明する。

【００７５】

まず、ＰＤ１２あるいはＬＣＭ１は、自身のデバイスＩＤをＭＣ１３へ転送する（ステップＳ１２１）。

【００７６】

ＬＣＭ１が図３に示すようなＰＤ２のコンテンツの再生機能部（復調部１２ｇ、デコーダ１２ｈ、Ｄ／Ａ変換部１２ｉ等）を持っているのであれば、ＭＣ１３をＰＤ１２で再生する場合もＬＣＭ１で再生する場合も同様であるので、以下、ＰＤ１２で再生する場合を例にとり説明する。

【００７７】

ＭＣ１３では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ１２２）、登録されていないとき秘匿領域１３ｃにアクセスしてマスターキーＫＭを読み出して、ＰＤ１２へ転送する（ステップＳ

１２３）。ＭＣ１３は、さらに、識別情報格納部１３ｂから、その識別情報（ＭＩＤ）を読み出して同じくＰＤ１２へ転送する（ステップＳ１２４）。

【００７８】

ＰＤ１２では、ＭＣ１３から転送されてきたメディアＩＤ（ＭＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＭＩＤ］）を生成する（ステップＳ１２５）。

【００７９】

ＰＤ１２では、この生成された情報ＫＭ［ＭＩＤ］を用いて相互認証処理（ＡＫＥ）を実行し、一方、ＭＣ１３でも秘匿メディアＩＤ（ＳＭＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（ステップＳ１２６）。ステップＳ１２６の相互認証処理（ＡＫＥ）は、図２１と同様であるので説明は省略する。

【００８０】

ＰＤ１２とＭＣ１３との間で相互に認証されたときは、ＭＣ１３では、生成した鍵情報ＫＴ（ここでは、ＫＴ２とする）を用いて秘匿領域１３ｃに格納されていた鍵情報ＫＴ１を暗号化して（ＫＴ２［ＫＴ１］）、ＰＤ１２へ転送する（ステップＳ１２７～ステップＳ１２８）。一方、ＰＤ１２では、ステップＳ１２６で生成された鍵情報ＫＴ２を用いてＭＣ１３から転送されてきたＫＴ２［ＫＴ１］を復号することができる（ステップＳ１２８）。

【００８１】

ＭＣ１３からは暗号化されたコンテンツ復号鍵ＫＴ１［Ｋｃ］、暗号化コンテンツＫｃ［Ｃ］を公開領域１３ａから読み出してＰＤ１２へ転送する（ステップＳ１２９、ステップＳ１３１）。

【００８２】

ＰＤ１２は、鍵情報ＫＴ１の復号に成功していれば、それを用いて暗号化されたコンテンツ復号鍵ＫＴ１［Ｋｃ］を復号してコンテンツ復号鍵Ｋｃが得られるので（ステップＳ１３０）、このコンテンツ復号鍵Ｋｃを用いて暗号化コンテンツＫｃ［Ｃ］を復号して、コンテンツＣを得る（ステップＳ１３２）。そして、ＰＤ１２では、コンテンツＣをデコーダ１２ｈでデコードして、Ｄ／Ａ変換部１２ｉでデジタル信号からアナログ信号に変換し、ＭＣ１３に記録されていた複製

コンテンツ（例えば音楽）を再生することができる。

【００８３】

次に、チェックインの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介して（すなわち、ＭＣ１３をＬＣＭ１に接続されたＰＤ１２にセットして用いた場合）、ＳＭＳ２になされた場合について、図１２を参照して説明する。

【００８４】

ＳＭＳ２は、デバイスＩＤ格納部４から当該ＬＣＭ１のデバイスＩＤ（ＬＣＭＩＤ）を読み出し、それをＭＣ１３へ転送する（ステップＳ１４１）。

【００８５】

ＭＣ１３では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ１４２）、登録されていないとき秘匿領域１３ｃにアクセスしてマスターキーＫＭを読み出して、ＬＣＭ１へ転送する（ステップＳ１４３）。ＭＣ１３は、さらに、識別情報格納部１３ｂから、その識別情報（ＭＩＤ）を読み出して同じくＬＣＭ１へ転送する（ステップＳ１４４）。

【００８６】

ＬＣＭ１では、ＭＣ１３から転送されてきたメディアＩＤ（ＭＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＭＩＤ］）を生成する（ステップＳ１４５）。

【００８７】

ＬＣＭ１では、この生成された情報ＫＭ［ＭＩＤ］を用いて相互認証処理（ＡＫＥ）を実行し、一方、ＭＣ１３でも秘匿メディアＩＤ（ＳＭＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（ステップＳ１４６）。

【００８８】

チェックインの際のステップＳ１４６の相互認証処理（ＡＫＥ）動作について、図２２を参照して説明する。なお、図２１と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図２２では、ステップＳ３０８で関数ｇの値が一致していたら、鍵情報ＫＴを生成する代わりに、フラグ情報Ｆａｋｅの値を「真」（図２２では「Ｔ」と示している）とし、不一致のときは「偽」（図

２２では「Ｆ」と示している）とする（ステップＳ３２１、ステップＳ３２２）。また、ＬＣＭ１では、ステップＳ３０４で関数ｇの値が一致していたら、鍵情報ＫＴを生成せずに、その判断結果のみを出力する。

【００８９】

図１２の説明に戻り、ステップＳ１４６において、ＬＣＭ１がＭＣ１３を認証したときには（図２２のステップＳ３０４）、ＭＣ１３に対し、その秘匿領域１３ｃに格納されている鍵情報ＫＴ１の削除を指示する。ＭＣ１３では、この指示を受けとると、フラグ情報Ｆａｋｅの値をチェックし、「Ｔ」であれば、秘匿領域１３ｃから鍵情報ＫＴ１を削除し、フラグ情報Ｆａｋｅを「Ｆ」に書き換える（ステップＳ１４７、ステップＳ１４８）。このとき、ＭＣ１３の公開領域１３ａに格納されている暗号化コンテンツ情報は、例えば、ＬＣＭ１にて発生した乱数にて上書きすることで消去してもよい。

【００９０】

最後に、図７（ｃ）に示すように、宿帳のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎに「１」加算し、チェックアウトリストＬ１から、当該ＭＣ１３の識別情報ｍ０を削除する。

【００９１】

一方、フラグ情報Ｆａｋｅの値が「Ｆ」のときは以降の処理を中止する。

【００９２】

次に、図１０とは異なる他のチェックアウト時の処理動作について、図１３を参照して説明する。なお、図１０と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図１３では、ＭＣ１３へ転送すべきコンテンツ復号鍵Ｋｃに対する処理に特徴がある。

【００９３】

図１３において、ＬＣＭ１３では、コンテンツ復号鍵Ｋｃに対し、まず、ステップＳ１０５で生成されたＫｍ［ＭＩＤ］（以下、これをｗと表す）を用いて暗号化を施す（ステップＳ１６２）。そして、ｗで暗号化されたコンテンツ復号鍵Ｋｃ（ｗ［Ｋｃ］）をステップＳ１０６の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いてさらに暗号化を行ってから（ＫＴ１［ｗ［Ｋｃ］］）、Ｍ

Ｃ１３へ転送する（ステップＳ１６３）。

【００９４】

ＭＣ１３では、ステップＳ１０６の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いて、転送されてきたＫＴ１［ｗ［Ｋｃ］］を復号してｗ［Ｋｃ］を得、これを秘匿領域１３へ格納する（ステップＳ１６４）。

【００９５】

コンテンツ情報Ｃは、図１０の場合と同様に、Ｋｃで暗号化してから（ステップＳ１６５）、ＭＣ１３へ転送される（ステップＳ１６６）。

【００９６】

図１３に示したようなチェックアウト処理動作に対応する再生処理動作について、図１４を参照して説明する。なお、図１１と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図１４において、ＭＣ１３は、秘匿領域１３ｃに格納されている暗号化コンテンツ復号鍵ｗ［Ｋｃ］をステップＳ１２６の相互認証処理（ＡＫＥ）で生成された鍵情報ＫＴ２で暗号化してから（ＫＴ２［ｗ［Ｋｃ］］）ＬＣＭ１あるいはＰＤ１２へ転送する。（ステップＳ１７２）。ＬＣＭ１あるいはＰＤ１２では、同じくステップＳ１２６で生成された鍵情報ＫＴ２でＭＣ１３から転送されてきたＫＴ２［ｗ［Ｋｃ］］を復号して（ステップＳ１７３）、その結果得られたｗ［Ｋｃ］をステップＳ１２３で生成されたｗ＝ＫＭ［ＭＩＤ］を用いて復号して、コンテンツ復号鍵Ｋｃを得る（ステップＳ１７４）。このコンテンツ復号鍵Ｋｃを用いて暗号化コンテンツＫｃ［Ｃ］を復号して、コンテンツＣを得る（ステップＳ１７５）。そして、ＬＣＭ１あるいはＰＤ１２では、コンテンツＣをデコーダ１２ｈでデコードして、Ｄ／Ａ変換部１２ｉでデジタル信号からアナログ信号に変換し、ＭＣ１３に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【００９７】

図１３に示したようなチェックアウト処理動作に対応するチェックイン処理動作は、図１２の説明とほぼ同様で、異なるのは、ステップＳ１４８でＭＣ１３の秘匿領域１３ｃから削除されるのは、鍵情報ＫＴ１ではなく、ｗ＝ＫＭ［ＭＩＤ］で暗号化されたコンテンツ復号鍵ｗ［Ｋｃ］であるという点である。

【００９８】

（３）レベル０のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

次に、図４（ａ）に示したような構成のレベル０のＭＣ１３を用いたチェックイン／チェックアウト、再生処理動作について説明する。

【００９９】

この場合、ＭＣ１３は、ＰＤ１２にセットされ、このＰＤ１２を介してＬＣＭ１との間でチェックアウト処理が実行される。基本的な動作は、ＭＣ１３がレベル２の場合と同様であるが、レベル０の場合、秘匿領域、メディアＩＤを有していないので、ＰＤ１２がＬＣＭ１に対する処理をレベル０のＭＣ１３に代行して図１０に示したような処理を実行することとなる。そのため、ＰＤ１２の秘匿領域には、マスターキーＫＭ、秘匿デバイスキーＳＰＤＩＤ、リボケーションリスト（ＲＶＣリスト）を予め記憶しておくものとする。なお、マスターキーＫＭは必ずしもメディアＭＣ１３に記憶しておくマスターキーＫＭとその機能は同じであるが、そのデータ自体は同じものである必要はない。

【０１００】

まず、図９のステップＳ３において、ＭＣ１３の種別がレベル０であると判定される。

【０１０１】

チェックアウトの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介してＳＭＳ２に対しなされた場合について、図１５を参照して説明する。

【０１０２】

ＳＭＳ２は、宿帳のチェックアウト要求のあったコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の子の残数ｎを調べ、ｎ＞０のとき、デバイスＩＤ格納部４から当該ＬＣＭ１のデバイスＩＤ（ＬＣＭＩＤ）を読み出し、それをＰＤ１２へ転送する（ステップＳ２０１）。

【０１０３】

ＰＤ１２では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ２０２）、登録されていないときＰＤ１２の秘匿領域にアクセスしてマスターキーＫＭを読み出して、ＬＣＭ１へ転送する（ステップＳ２０３）。ＰＤ１２は、さらに、例えばＲＯＭ１２ｃからその識別情報、すなわち、デバイスＩＤ（ＰＤＩＤ）を読み出して、同じくＬＣＭ１へ転送する（ステップＳ２０４）。

【０１０４】

ＬＣＭ１では、ＰＤ１２から転送されてきたデバイスＩＤ（ＰＤＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＰＤＩＤ］）を生成する（ステップＳ２０５）。

【０１０５】

ＬＣＭ１では、この生成された情報ＫＭ［ＰＤＩＤ］を用いて相互認証処理（ＡＫＥ）を実行し、一方、ＰＤ１２でも秘匿デバイスＩＤ（ＳＰＤＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（ステップＳ２０６）。ステップＳ２０６の相互認証処理（ＡＫＥ）は、図２１と同様であるので説明は省略する。

【０１０６】

ＬＣＭ１とＰＤ１２との間で相互に認証されたとき、ＰＤ１２では、生成した鍵情報ＫＴ（ここでは、ＫＴ１とする）を秘匿領域に格納する（ステップＳ２０７）。ＬＣＭ１では、暗号化コンテンツを復号するための復号鍵（コンテンツ復号鍵）Ｋｃをステップ２０６で生成された鍵情報ＫＴ１で暗号化して（ＫＴ１［Ｋｃ］）、ＰＤ１２を経由してＭＣ１３へ転送し（ステップＳ２０８～ステップＳ２０９）、また、コンテンツ情報ＣをＫｃで暗号化して（Ｋｃ［Ｃ］）、ＰＤ１２を経由してＭＣ１３へ転送する（ステップＳ２１０～ステップＳ２１１）。

【０１０７】

最後に、ＳＭＳ２は、図７（ｂ）に示すように、宿帳のチェックアウト要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎから「１」減算し、チェックアウトリストＬ１に、当該ＭＣ１３の識別情報「ｍ０」を追加する。

【０１０８】

ＭＣ１３は、転送されてきた暗号化されたコンテンツ復号鍵ＫＴ１［Ｋｃ］、暗号化コンテンツＫｃ［Ｃ］を公開領域１３ａに格納する。

【０１０９】

以上の処理が終了したときのＭＣ１３の記憶内容を図６に示す。

【０１１０】

次に、再生の指示がＰＤ１２に対しなされた場合のＰＤ１２とＭＣ１３との間の処理動作について、図１６を参照して説明する。

【０１１１】

まず、ＭＣ１３は、公開領域に記録されている暗号化されたコンテンツ復号鍵ＫＴ１［Ｋｃ］をＰＤ１２へ転送する（ステップＳ２２１）。ＰＤ１２が当該ＭＣ１３に対し当該再生対象のコンテンツ情報をチェックアウトした際に用いたものであるならば、その秘匿領域に暗号化されたコンテンツ復号鍵を復号するための鍵情報ＫＴ１を記憶している（図１５のステップＳ２０７参照）。従って、そのような正当なＰＤ１２であるならば、秘匿領域から読み出した鍵情報ＫＴ１を用いて、ＭＣ１３から転送されてきたＫＴ１［Ｋｃ］を復号して、コンテンツ復号鍵Ｋｃを得ることができる（ステップＳ２２２）。さらに、このコンテンツ復号鍵Ｋｃを用いて、ＭＣ１３から転送されてきた暗号化コンテンツ情報Ｋｃ［Ｃ］を復号してコンテンツＣを得ることができる（ステップＳ２２３～ステップＳ２２４）。そして、ＰＤ１２では、コンテンツＣをデコーダ１２ｈでデコードして、Ｄ／Ａ変換部１２ｉでデジタル信号からアナログ信号に変換し、ＭＣ１３に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【０１１２】

次に、チェックインの指示がＰＤ１２を介して（すなわち、ＭＣ１３をＬＣＭ１に接続されたＰＤ１２にセットして用いて）、ＳＭＳ２になされた場合について、図１７を参照して説明する。この場合もチェックアウトの場合と同様、ＰＤ１２がＬＣＭ１に対する処理をレベル０のＭＣ１３に代行して図１２に示したような処理を実行することとなる。

【０１１３】

ＳＭＳ２は、デバイスＩＤ格納部４から当該ＬＣＭ１のデバイスＩＤ（ＬＣＭ

ＩＤ）を読み出し、それをＰＤ１２へ転送する（ステップＳ２３１）。

【０１１４】

ＰＤ１２では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ２３２）、登録されていないとき秘匿領域にアクセスしてマスターキーＫＭを読み出して、ＬＣＭ１へ転送する（ステップＳ２３３）。ＰＤ１２は、さらに、その識別情報（ＰＤＩＤ）を読み出して同じくＬＣＭ１へ転送する（ステップＳ２３４）。

【０１１５】

ＬＣＭ１では、ＰＤ１２から転送されてきたデバイスＩＤ（ＰＤＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＰＤＩＤ］）を生成する（ステップＳ２３５）。

【０１１６】

ＬＣＭ１では、この生成された情報ＫＭ［ＰＤＩＤ］を用いて相互認証処理（ＡＫＥ）を実行し、一方、ＰＤ１２でも秘匿デバイスＩＤ（ＳＰＤＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（ステップＳ２３６）。

【０１１７】

チェックインの際のステップＳ２３６の相互認証処理（ＡＫＥ）動作は、図２２において、ＫＭ［ＭＩＤ］をＫＭ［ＰＤＩＤ］に置き換え、秘匿メディアＩＤ（ＳＭＩＤ）が秘匿デバイスＩＤ（ＳＰＤＩＤ）に置き換えれば同様であるので、説明は省略する。

【０１１８】

ステップＳ２３６において、ＬＣＭ１がＰＤ１２を認証したときには（図２２のステップＳ３０４）、ＰＤ１２に対し、その秘匿領域に格納されている鍵情報ＫＴ１の削除を指示する。ＰＤ１２では、この指示を受けとると、フラグ情報Ｆａｋｅの値をチェックし、「Ｔ」であれば、秘匿領域から鍵情報ＫＴ１を削除し、フラグ情報Ｆａｋｅを「Ｆ」に書き換える（ステップＳ２３７、ステップＳ２３８）。このとき、ＭＣ１３の公開領域１３ａに格納されている暗号化コンテンツ情報は、例えば、ＬＣＭ１にて発生した乱数にて上書きすることで消去してもよい。

【０１１９】

最後に、図７（ｃ）に示すように、宿帳のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎに「１」加算し、チェックアウトリストＬ１から、当該ＭＣ１３の識別情報ｍ０を削除する。

【０１２０】

一方、フラグ情報Ｆａｋｅの値が「Ｆ」のときは以降の処理を中止する。

【０１２１】

次に、図１５とは異なる他のチェックアウト時の処理動作について、図１８を参照して説明する。なお、図１５と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図１８では、図１３の場合と同様に、ＰＤ１２へ転送すべきコンテンツ復号鍵Ｋｃに対する処理に特徴がある。

【０１２２】

図１８において、ＬＣＭ１３では、コンテンツ復号鍵Ｋｃに対し、まず、ステップＳ２０５で生成されたＫｍ［ＰＤＩＤ］（以下、これをｗと表す）を用いて暗号化を施す（ステップＳ２５２）。そして、ｗで暗号化されたコンテンツ復号鍵Ｋｃ（ｗ［Ｋｃ］）をステップＳ２５１の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いてさらに暗号化を行ってから（ＫＴ１［ｗ［Ｋｃ］］）、ＰＤ１２へ転送する（ステップＳ２５３）。

【０１２３】

ＰＤ１２では、ステップＳ２５１の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いて、転送されてきたＫＴ１［ｗ［Ｋｃ］］を復号してｗ［Ｋｃ］を得、これを秘匿領域へ格納する（ステップＳ２５４）。

【０１２４】

コンテンツ情報Ｃは、図１５の場合と同様に、Ｋｃで暗号化してから（ステップＳ２５５）、ＰＤ１２を経由してＭＣ１３へ転送される（ステップＳ２５６）。

【０１２５】

図１８に示したようなチェックアウト処理動作に対応する再生処理動作について、図１９を参照して説明する。なお、図１８と同一部分には同一符号を付し、

異なる部分についてのみ説明する。すなわち、図１９において、ＰＤ１２は、自身の秘匿領域に格納されている暗号化コンテンツ復号鍵ｗ［Ｋｃ］を同じく自身の秘匿デバイスＩＤ（ＳＰＤＩＤ＝ｗ）を用いて復号し、コンテンツ復号鍵Ｋｃを得ることができる（ステップＳ２６１）。このコンテンツ復号鍵Ｋｃを用いてＭＣ１３から転送されてきた暗号化コンテンツＫｃ［Ｃ］を復号して、コンテンツＣを得ることができる（ステップＳ２６２）。そして、ＰＤ１２では、コンテンツＣをデコーダ１２ｈでデコードして、Ｄ／Ａ変換部１２ｉでデジタル信号からアナログ信号に変換し、ＭＣ１３に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【０１２６】

図１８に示したようなチェックアウト処理動作に対応するチェックイン処理動作について、図２０を参照して説明する。なお、図２０の説明は、図１７の説明とほぼ同様で、異なるのは、ステップＳ２３８でＰＤ１２の秘匿領域から削除されるのは、鍵情報ＫＴ１ではなく、ｗ＝ＫＭ［ＰＤＩＤ］で暗号化されたコンテンツ復号鍵ｗ［Ｋｃ］であるという点である。

【０１２７】

【発明の効果】

以上説明したように、本発明によれば、低コストな記録媒体を用いて、セキュリティ性の高い安全な相互認証が実現できる。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る記憶媒体（メディア）に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム（ＬＣＭ）の構成例を示した図。

【図２】

メモリ領域の構成例を示した図。

【図３】

記録再生装置（ＰＤ）の内部構成例を示した図。

【図４】

３種類の記憶媒体の特徴を説明するための図。

【図５】

メディアインタフェース（Ｉ／Ｆ）部の内部構成例を示した図。

【図６】

チェックイン後の記憶媒体の記録内容を説明するための図。

【図７】

ＬＣＭの秘匿領域に格納されている宿帳の記憶例を示した図。

【図８】

相互認証方法の概略を説明するための図。

【図９】

チェックイン／チェックアウト処理手順を説明するためのフローチャートで、メディアの種別を判別して、その種別に応じた処理を選択するまでの手順を示したものである。

【図１０】

記録媒体の種別がレベル２の場合のチェックアウト時の手順を説明するための図。

【図１１】

記録媒体の種別がレベル２の場合の再生時の手順を説明するための図。

【図１２】

記録媒体の種別がレベル２の場合のチェックイン時の手順を説明するための図。

【図１３】

記録媒体の種別がレベル２の場合のチェックアウト時の他の手順を説明するための図。

【図１４】

記録媒体の種別がレベル２の場合の再生時の他の手順を説明するための図。

【図１５】

記録媒体の種別がレベル０の場合のチェックアウト時の手順を説明するための図。

【図１６】

記録媒体の種別がレベル０の場合の再生時の手順を説明するための図。

【図１７】

記録媒体の種別がレベル０の場合のチェックイン時の手順を説明するための図。

【図１８】

記録媒体の種別がレベル０の場合のチェックアウト時の他の手順を説明するための図。

【図１９】

記録媒体の種別がレベル０の場合の再生時の他の手順を説明するための図。

【図２０】

記録媒体の種別がレベル２の場合のチェックイン時の他の手順を説明するための図。

【図２１】

相互認証処理（ＡＫＥ）の処理動作について説明するための図。

【図２２】

相互認証処理（ＡＫＥ）の他の処理動作について説明するための図。

【符号の説明】

１…ＬＣＭ（コンテンツ利用管理システム）

２…ＳＭＳ（セキュア・コンテンツ・サーバ）

３…ＥＭＤインタフェース部

４…デバイスＩＤ格納部

５…ＰＤインタフェース部

６…メディアインタフェース部

７…秘匿領域ドライバ

８…宿帳格納部

９…ライセンス格納部

１０…音楽データ格納部

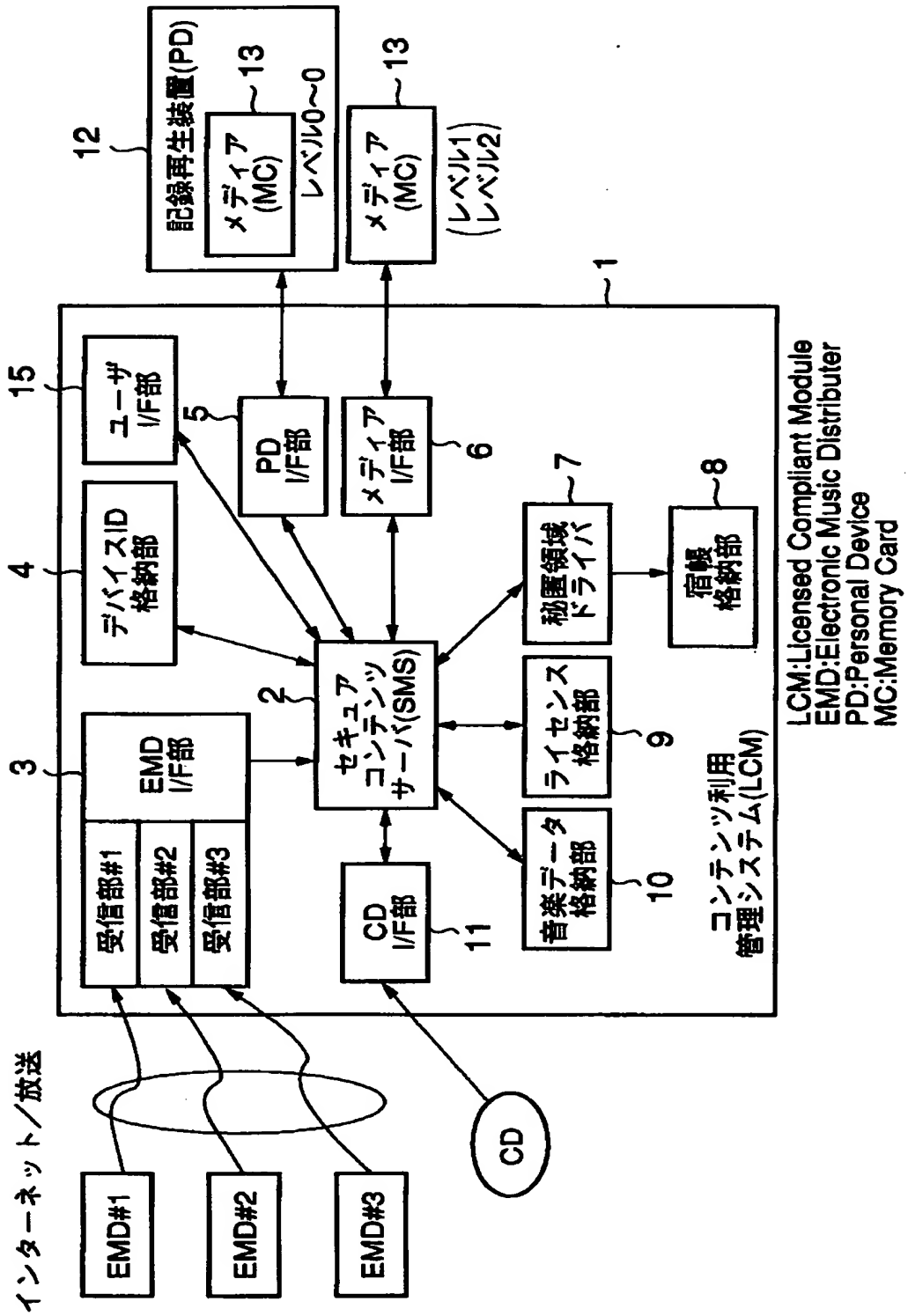
１１…ＣＤインタフェース部

１２…ＰＤ（記録再生装置）

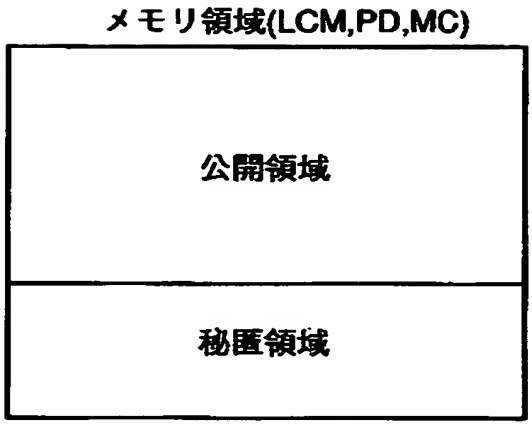
１３…ＭＣ（記録媒体、メディア）

【書類名】　　図面

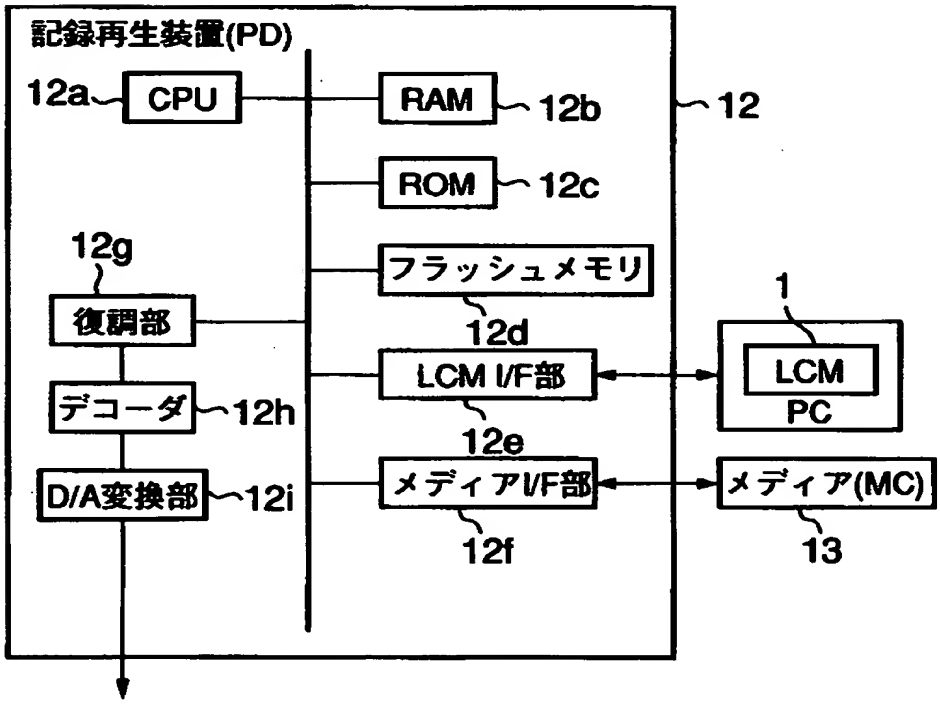
【図１】


インターネット／放送
EMD#1
EMD#2
EMD#3
CD
受信部#1
受信部#2
受信部#3
EMD I/F部
CD I/F部
セキュア コンテンツ サーバ(SMS)
PD I/F部
メディア I/F部
ユーザ I/F部
デバイスID 格納部
秘匿領域 ドライバ
宿帳 格納部
ライセンス 格納部
音楽データ 格納部
コンテンツ利用 管理システム(LCM)
記録再生装置(PD)
メディア (MC)
レベル0～0
メディア (MC)
(レベル1 レベル2)
1
2
3
4
5
6
7
8
9
10
11
12
13
13
15
LCM:Licensed Compliant Module
EMD:Electronic Music Distributer
PD:Personal Device
MC:Memory Card

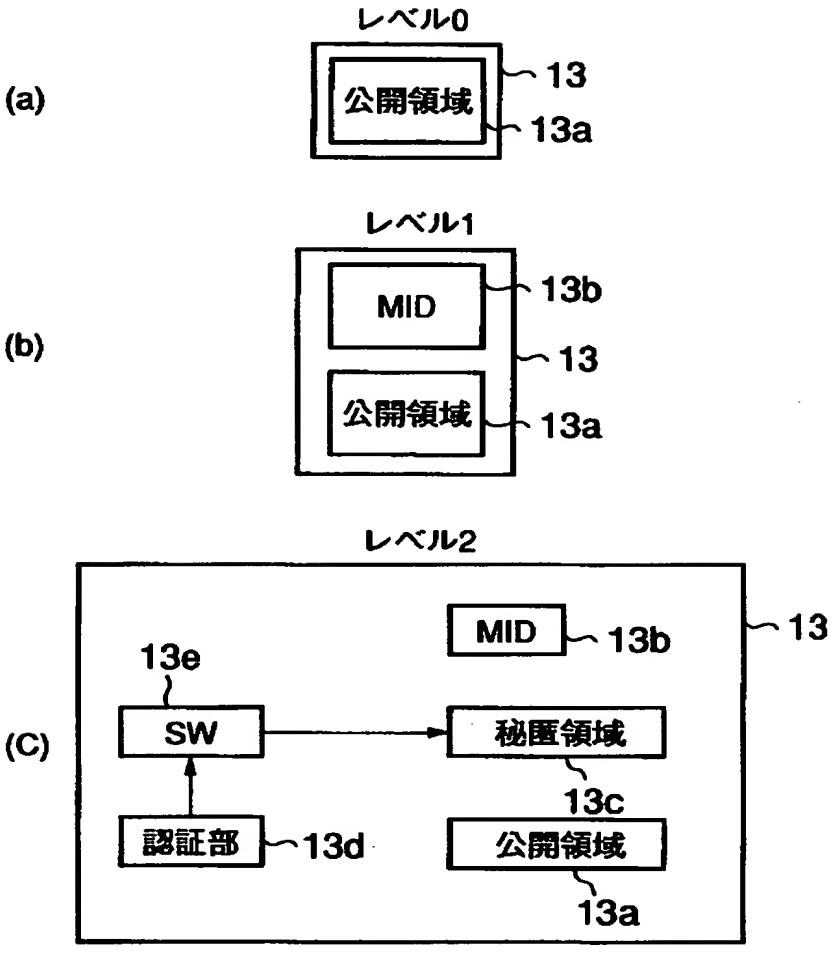
【図２】


メモリ領域(LCM,PD,MC)
公開領域
秘匿領域

【図３】

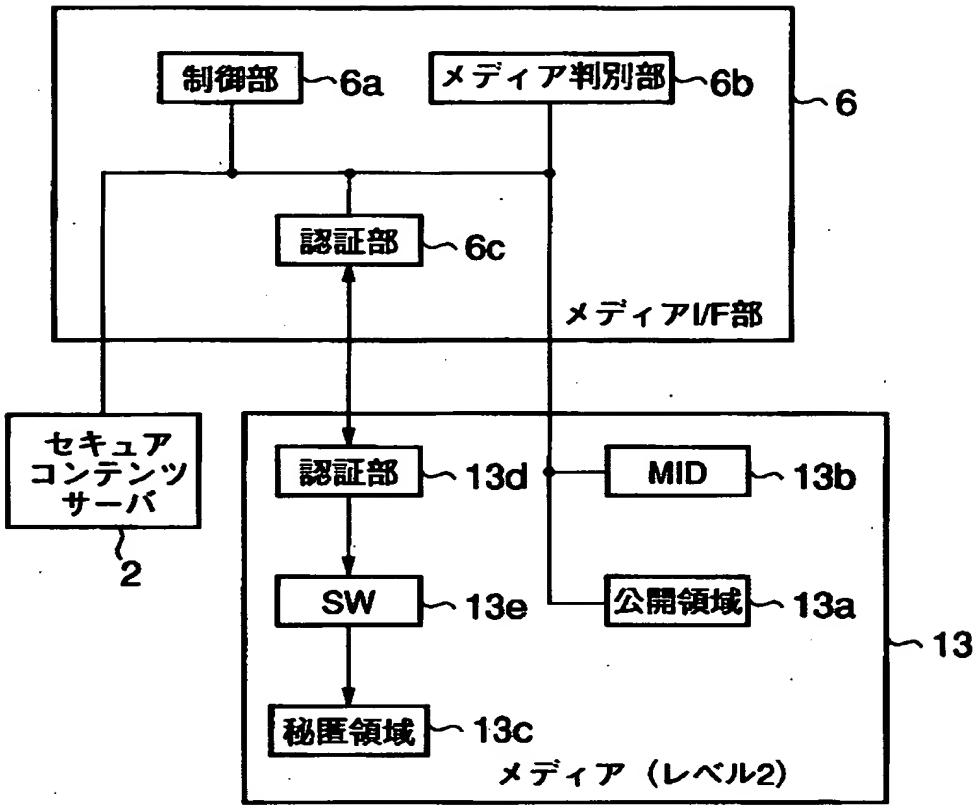

記録再生装置(PD)
12a
CPU
RAM
12b
12
ROM
12c
12g
フラッシュメモリ
1
復調部
12d
LCM I/F部
LCM
PC
デコーダ
12h
12e
D/A変換部
12i
メディアI/F部
メディア(MC)
12f
13

【図４】

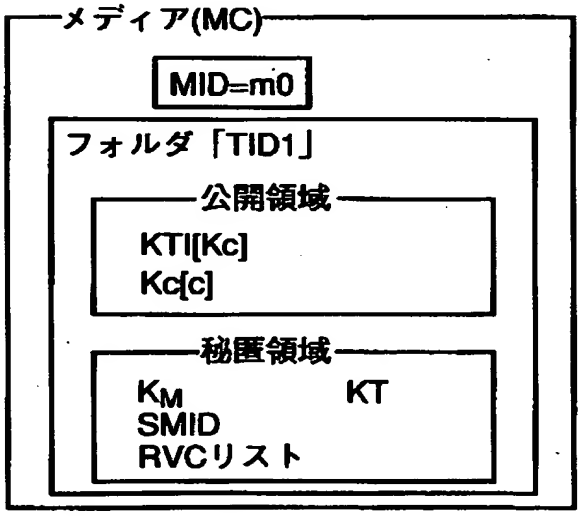


出証特２０００－３０４６６７５

【図５】

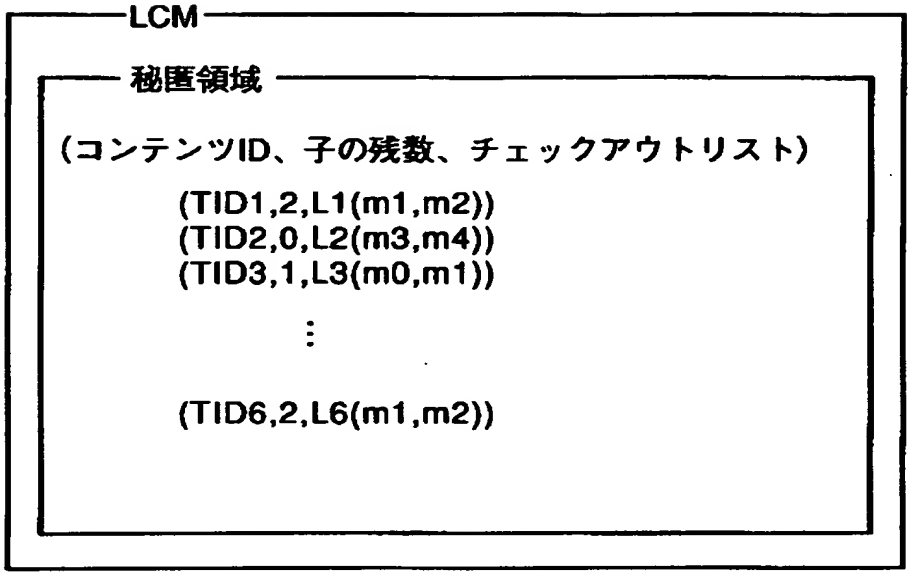

制御部
6a
メディア判別部
6b
6
認証部
6c
メディアI/F部
セキュア
コンテンツ
サーバ
2
認証部
13d
MID
13b
SW
13e
公開領域
13a
13
秘匿領域
13c
メディア（レベル2）

【図６】

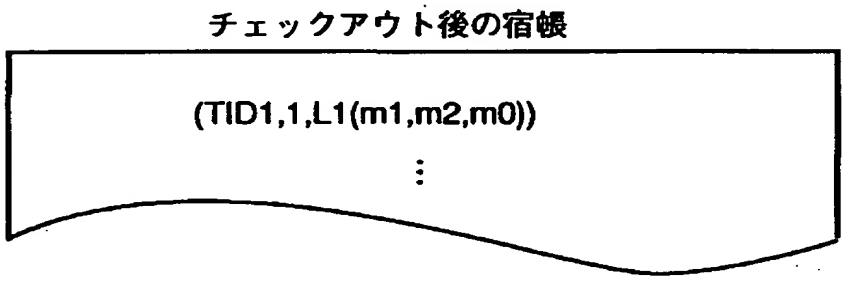

メディア(MC)
MID=m0
フォルダ「TID1」
公開領域
KTI[Kc]
Kc[c]
秘匿領域
KM
KT
SMID
RVCリスト

【図７】

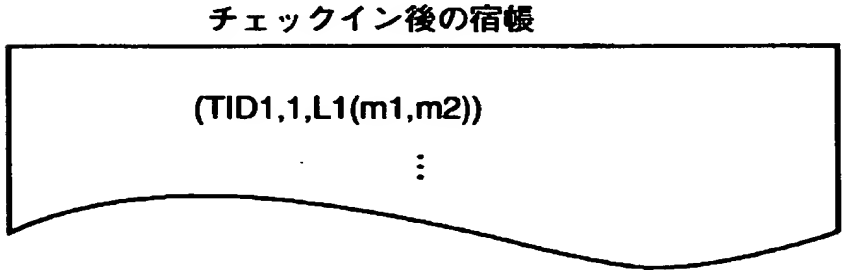
(a)


LCM
秘匿領域
(コンテンツID、子の残数、チェックアウトリスト)
(TID1,2,L1(m1,m2))
(TID2,0,L2(m3,m4))
(TID3,1,L3(m0,m1))
(TID6,2,L6(m1,m2))

(b)

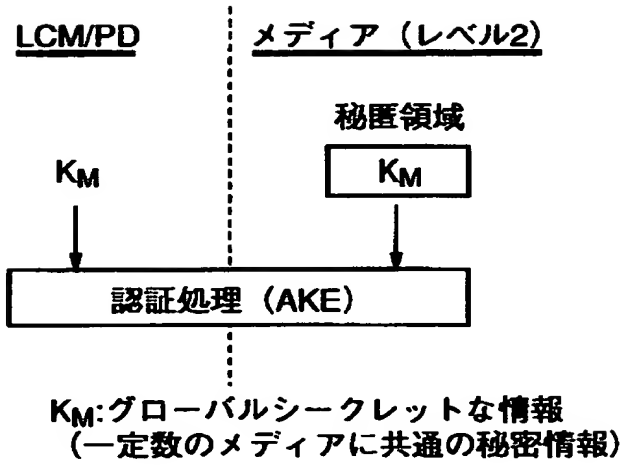

チェックアウト後の宿帳
(TID1,1,L1(m1,m2,m0))

(c)


チェックイン後の宿帳
(TID1,1,L1(m1,m2))

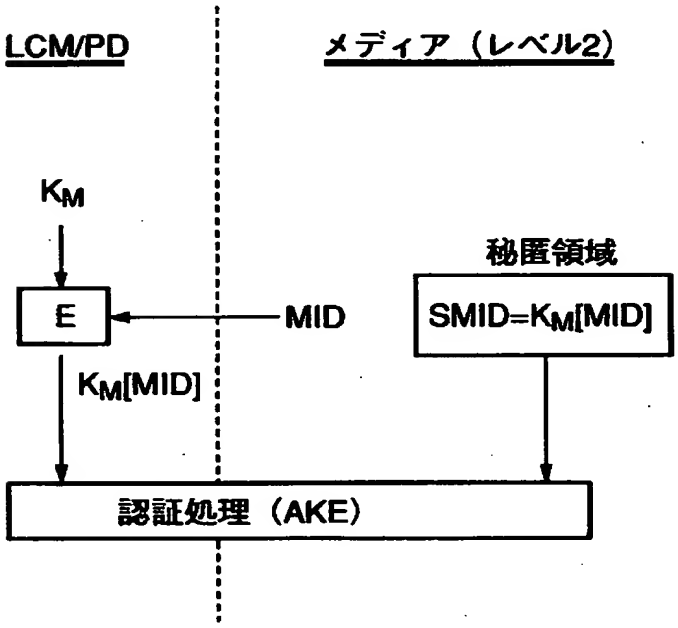
【図８】

(a)

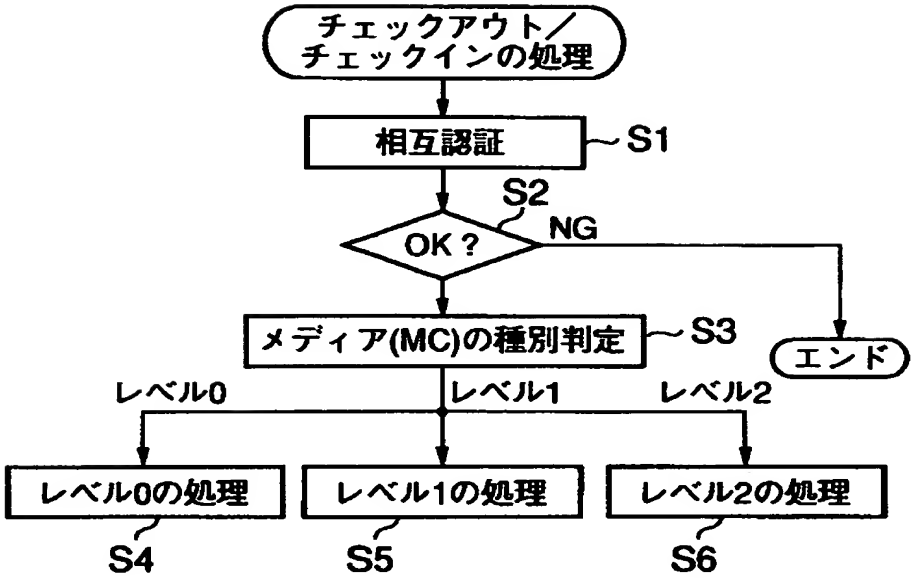


K_M:グローバルシークレットな情報
（一定数のメディアに共通の秘密情報）

(b)

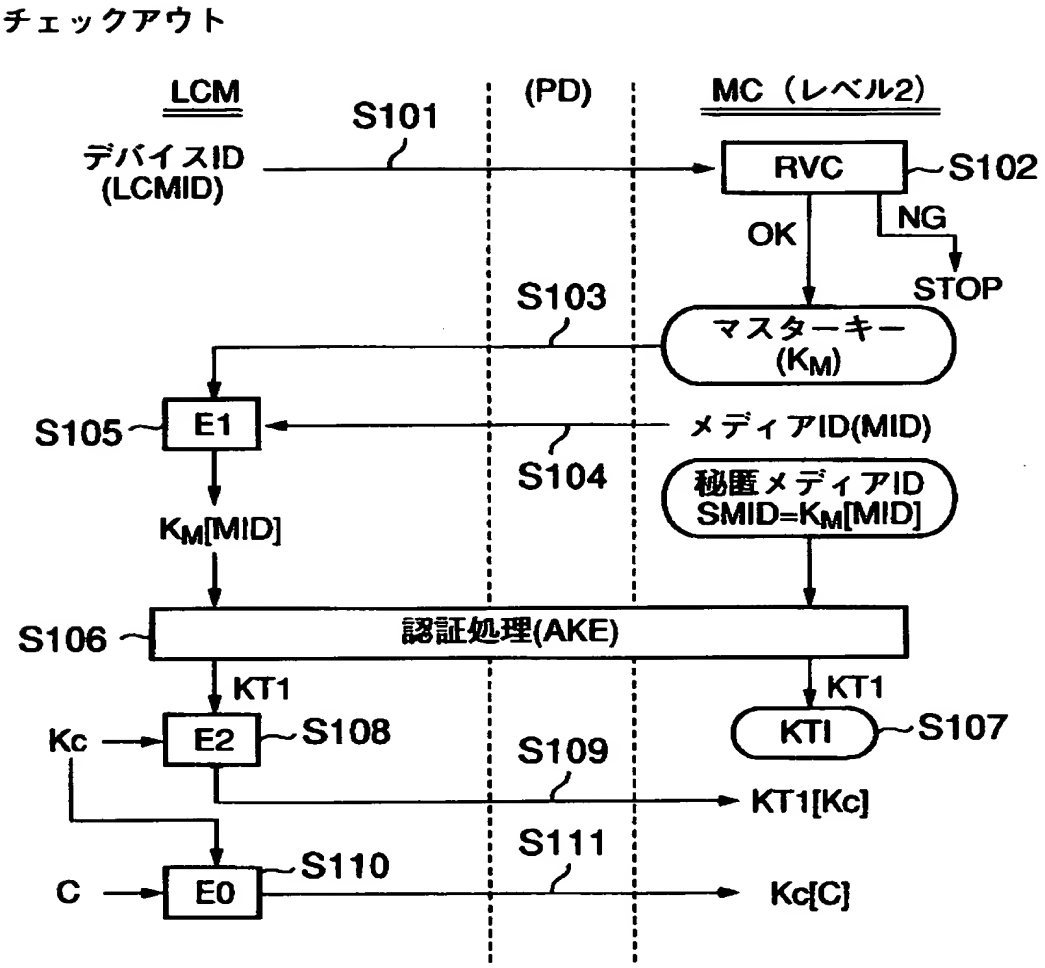


【図９】



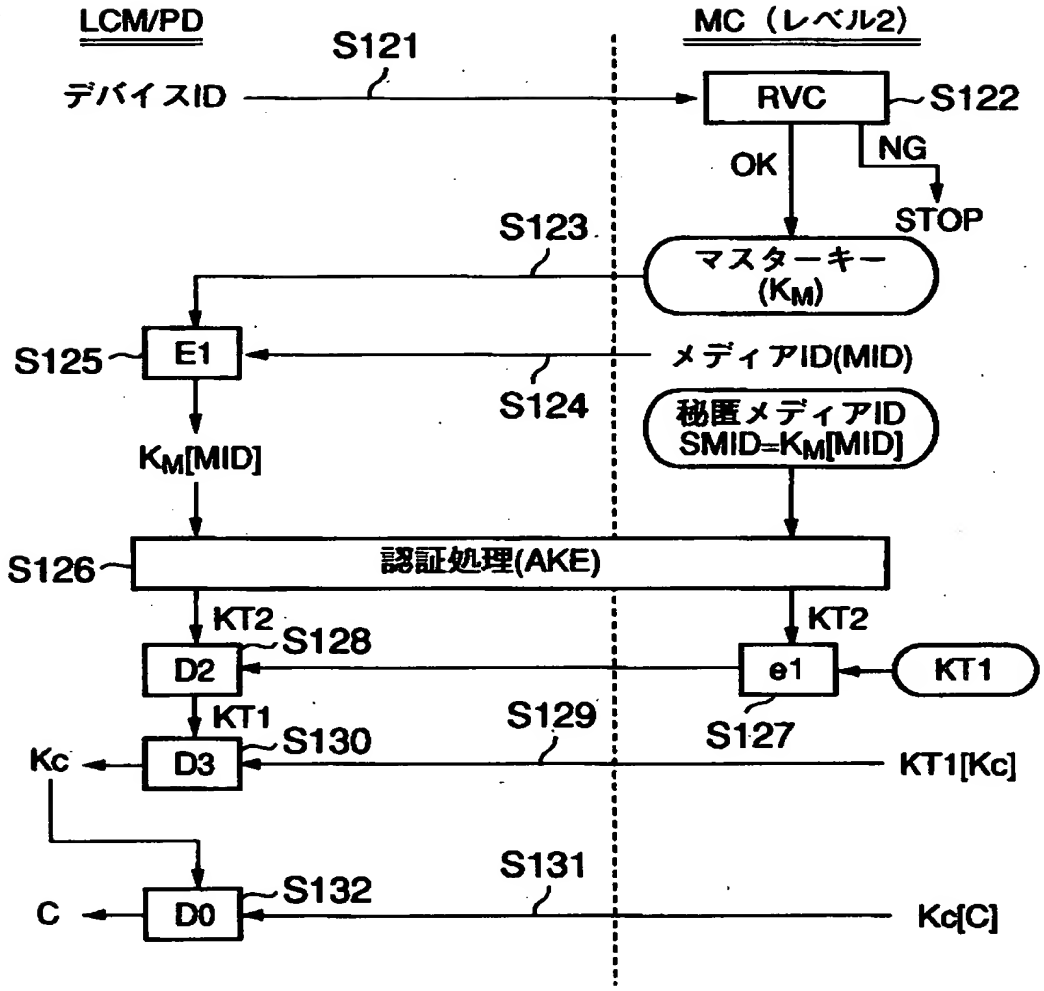
出証特２０００－３０４６６７５

【図１０】

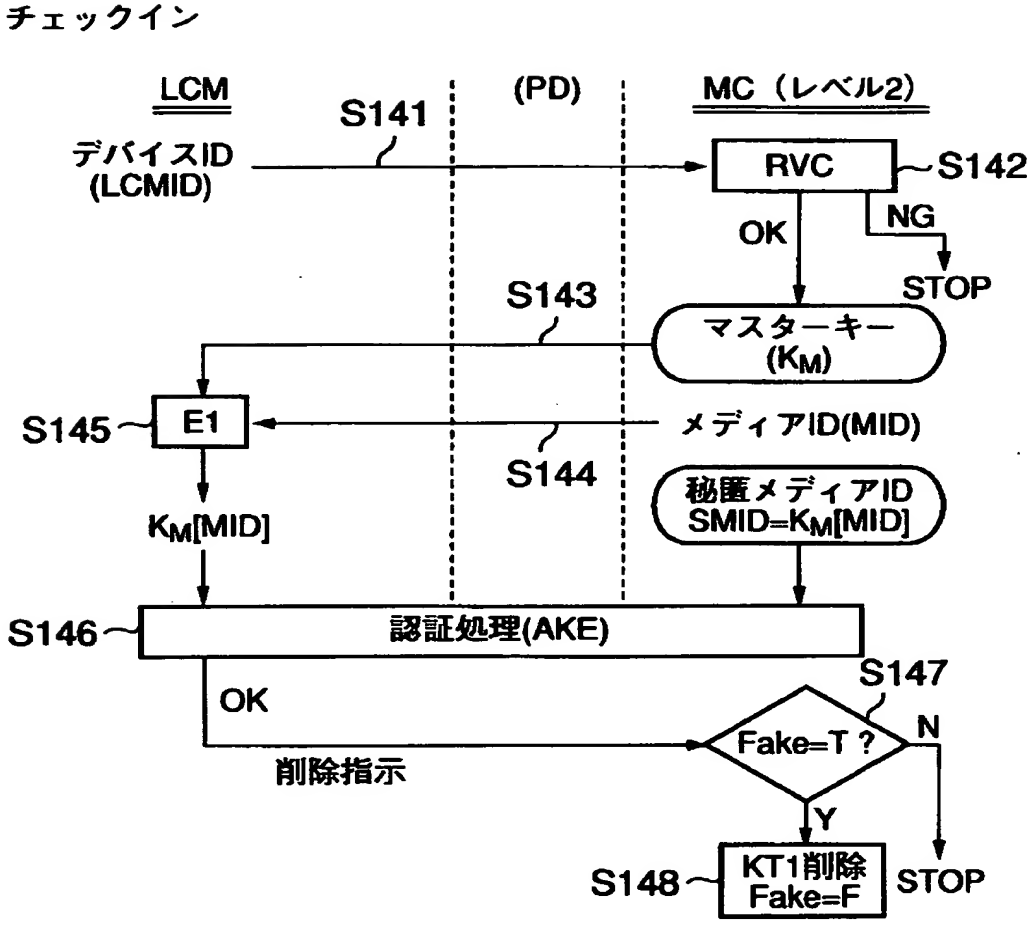

チェックアウト
LCM
(PD)
MC（レベル2）
S101
デバイスID
(LCMID)
RVC
S102
OK
NG
STOP
S103
マスターキー
(KM)
S105
E1
メディアID(MID)
S104
秘匿メディアID
SMID=KM[MID]
KM[MID]
S106
認証処理(AKE)
KT1
KT1
Kc
E2
S108
KTI
S107
S109
KT1[Kc]
S111
S110
C
E0
Kc[C]

【図１１】

再生

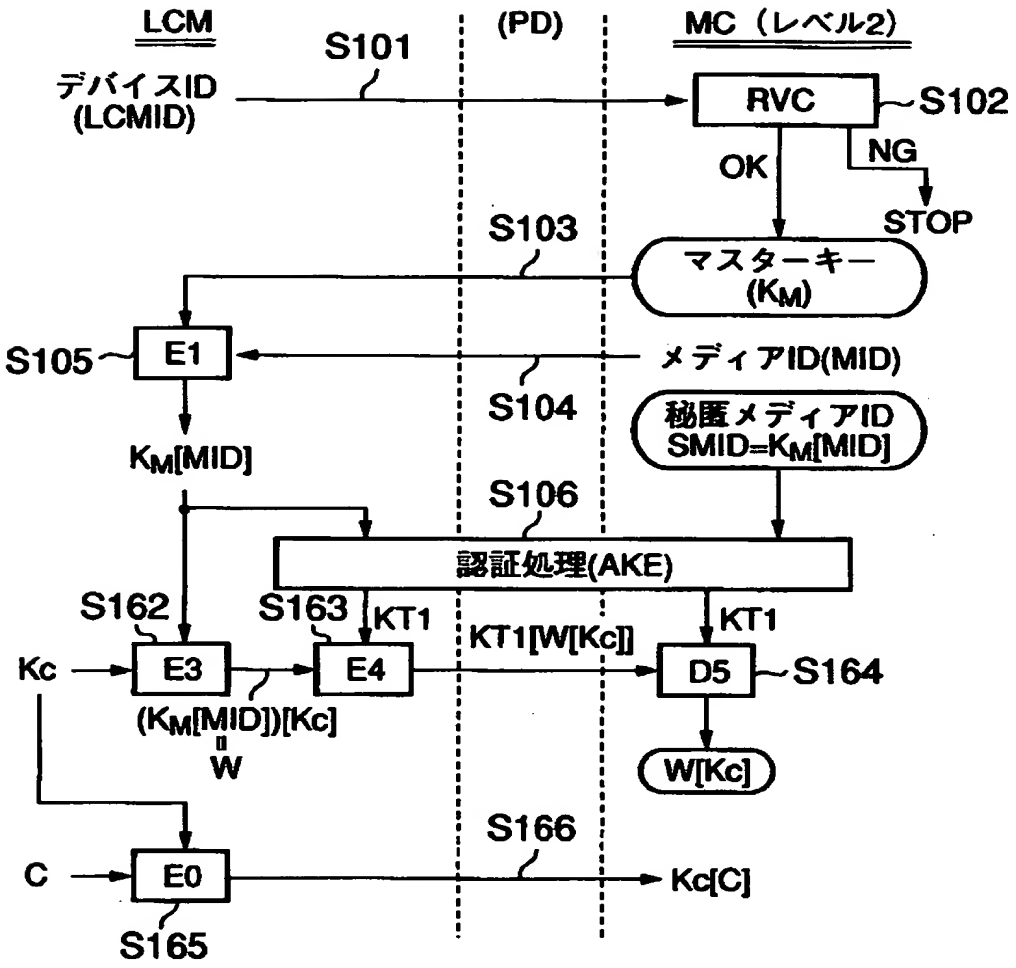

LCM/PD
MC（レベル2）
S121
デバイスID
RVC
S122
OK
NG
STOP
S123
マスターキー
(KM)
S125
E1
メディアID(MID)
S124
秘匿メディアID
SMID=KM[MID]
KM[MID]
S126
認証処理(AKE)
KT2
KT2
S128
D2
e1
KT1
KT1
S129
S127
S130
Kc
D3
KT1[Kc]
S131
S132
C
D0
Kc[C]

【図１２】

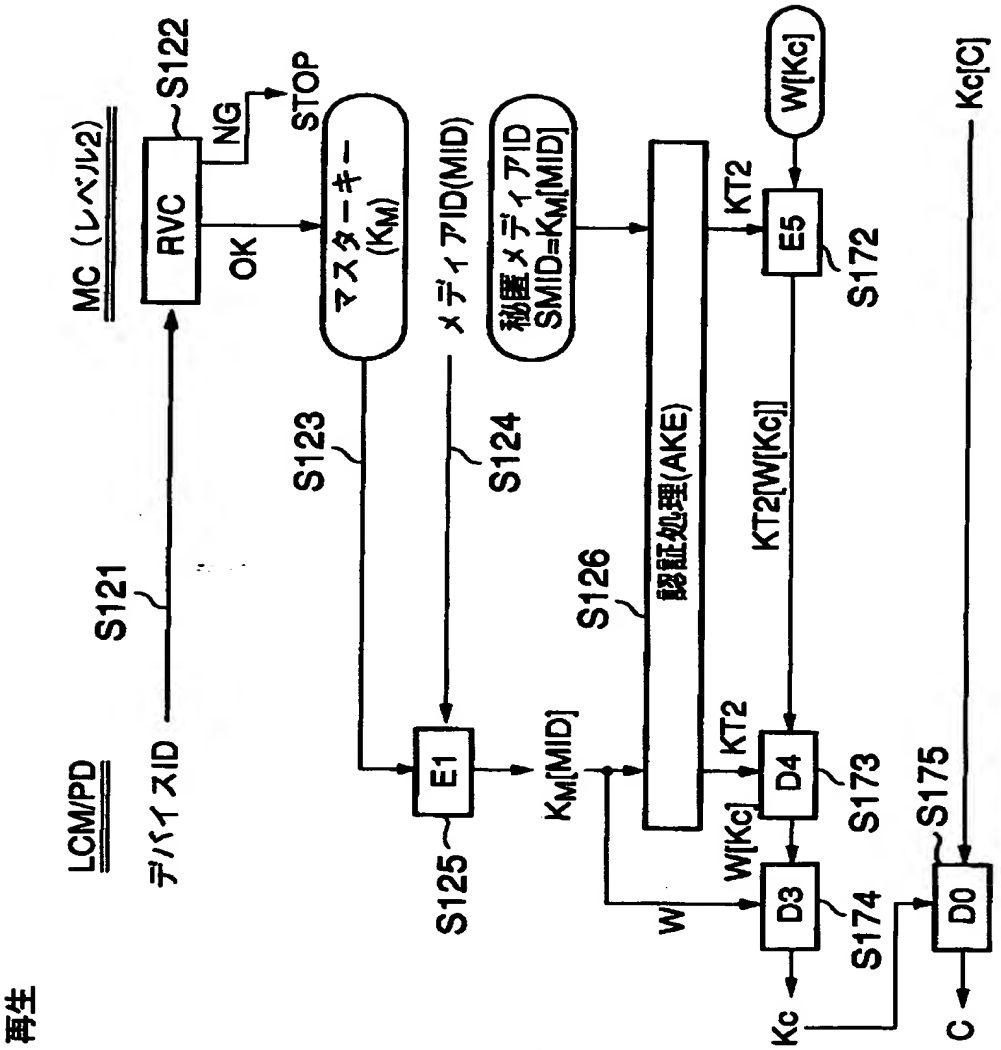

チェックイン
LCM
(PD)
MC（レベル2）
S141
デバイスID
(LCMID)
RVC
S142
OK
NG
STOP
S143
マスターキー
(KM)
S145
E1
メディアID(MID)
S144
秘匿メディアID
SMID=KM[MID]
KM[MID]
S146
認証処理(AKE)
S147
OK
Fake=T？
N
削除指示
Y
S148
KT1削除
Fake=F
STOP

【図１３】

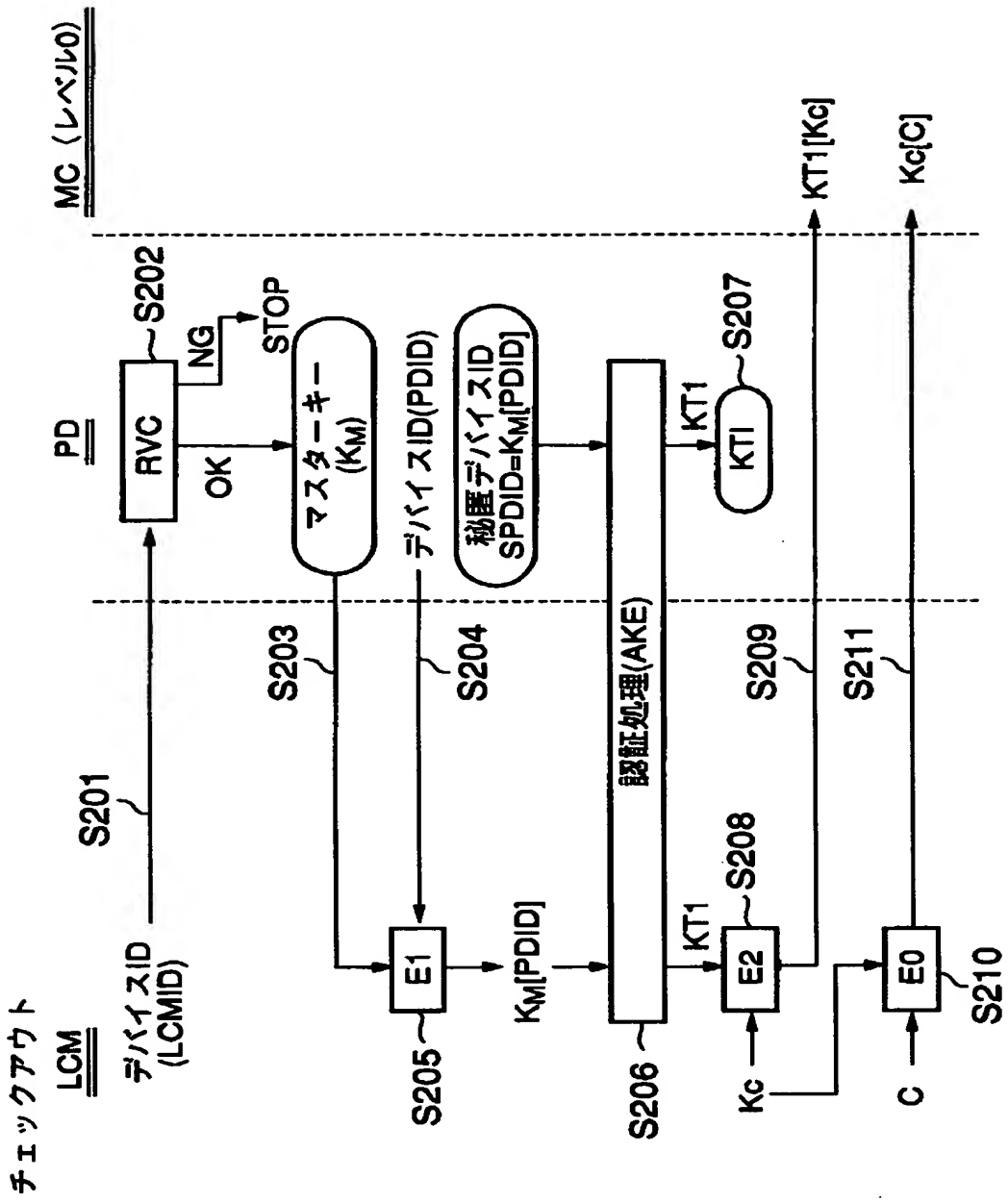
チェックアウト


LCM
(PD)
MC（レベル2）
S101
デバイスID
(LCMID)
RVC
S102
OK
NG
STOP
S103
マスターキー
(KM)
S105
E1
メディアID(MID)
S104
秘匿メディアID
SMID=KM[MID]
KM[MID]
S106
認証処理(AKE)
S162
S163
KT1
KT1
KT1[W[Kc]]
Kc
E3
E4
D5
S164
(KM[MID])[Kc]
W
W[Kc]
S166
C
E0
Kc[C]
S165

【図１４】

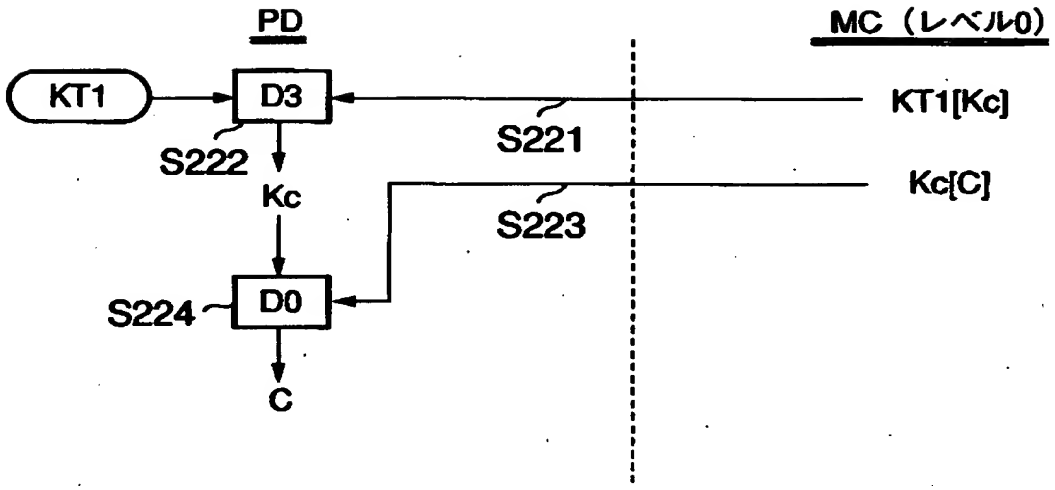

再生
LCM/PD
デバイスID
S121
MC（レベル2）
RVC
S122
NG
STOP
OK
マスターキー
(K_M)
S123
メディアID(MID)
S124
秘匿メディアID
SMID=K_M[MID]
S126
認証処理(AKE)
W[Kc]
KT2
E5
S172
KT2[W[Kc]]
Kc[C]
E1
S125
K_M[MID]
KT2
D4
S173
W[Kc]
D3
S174
W
D0
S175
Kc
C

【図１５】

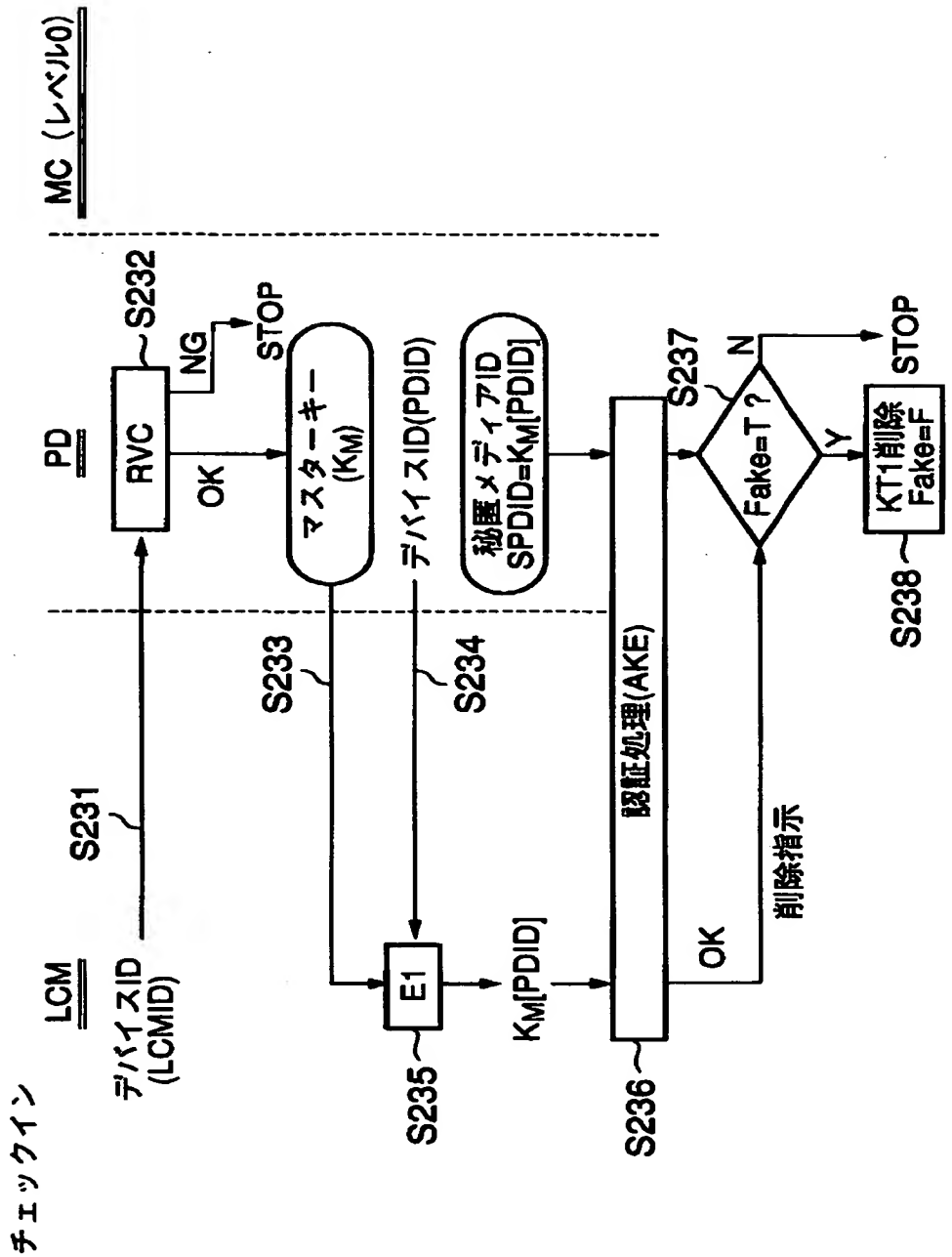

MC（レベル0）
PD
LCM
チェックアウト
デバイスID
(LCMID)
S201
RVC
S202
NG
STOP
OK
マスターキー
(KM)
S203
デバイスID(PDID)
S204
秘匿デバイスID
SPDID=KM[PDID]
E1
S205
KM[PDID]
認証処理(AKE)
S206
KT1
S207
KT1
S208
E2
KC
S209
KT1[Kc]
S211
Kc[C]
E0
C
S210

【図１６】

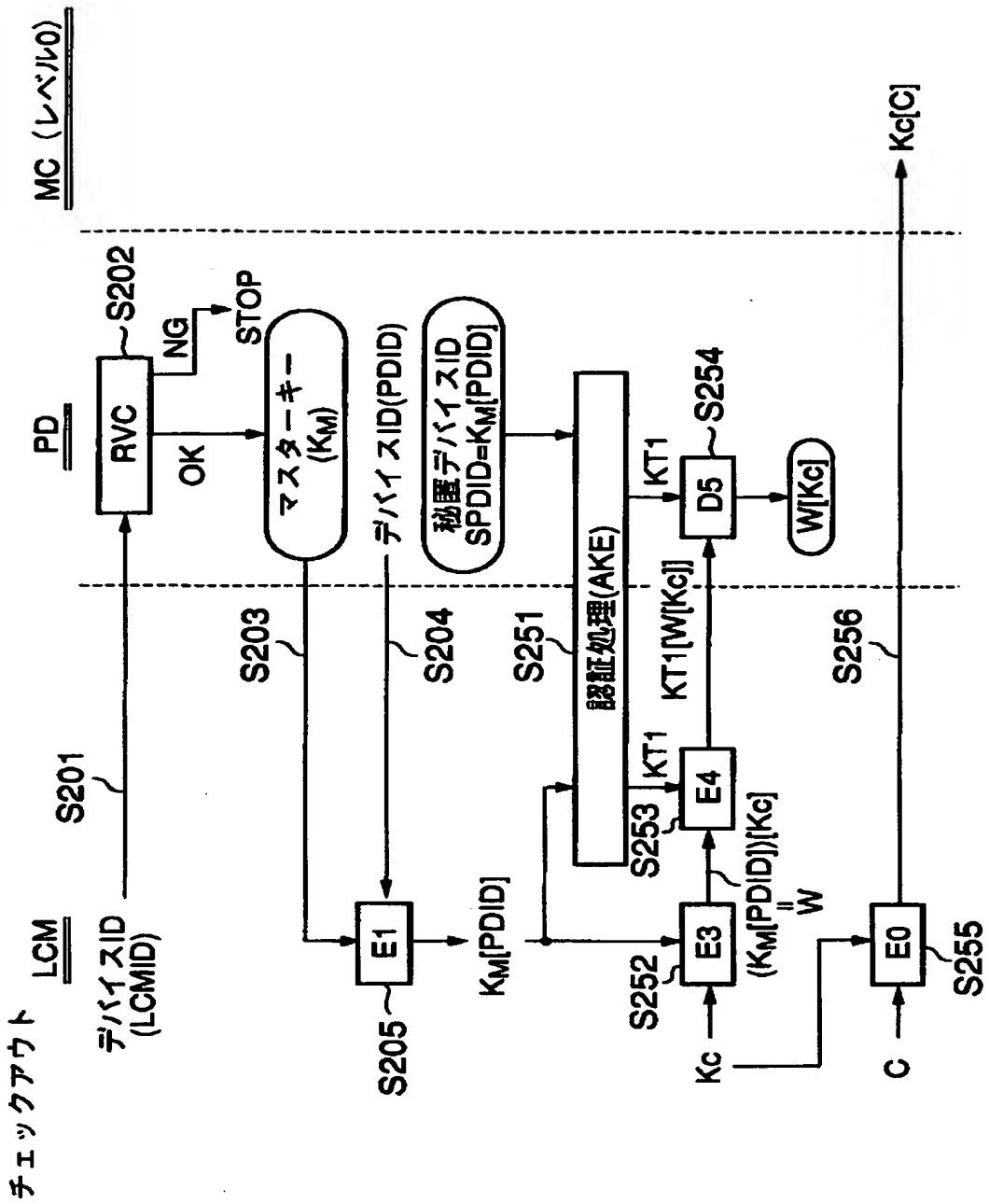
再生



【図１７】

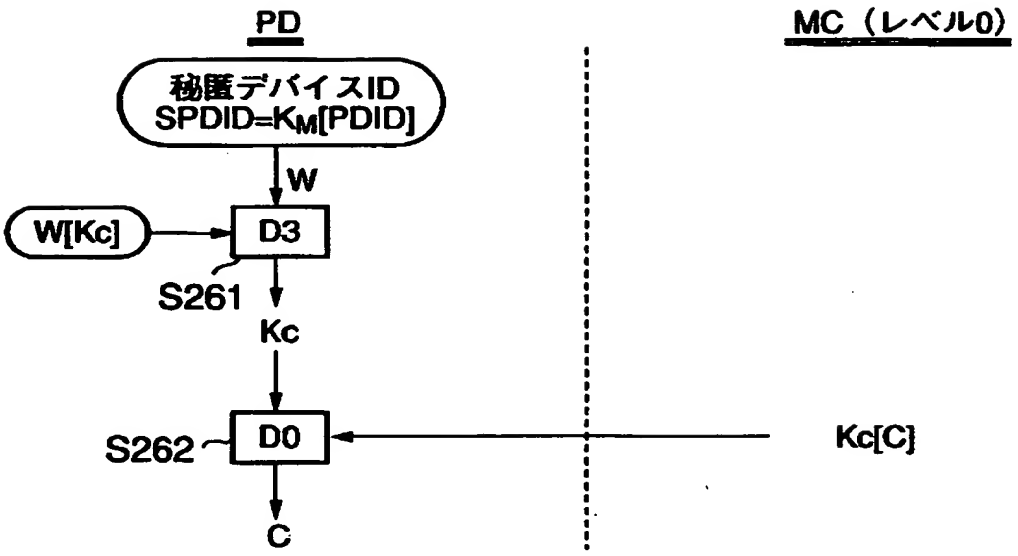

MC (レベル0)
PD
RVC
S232
NG
STOP
OK
マスターキー
(KM)
デバイスID(PDID)
秘匿メディアID
SPDID=KM[PDID]
S237
N
Fake=T ?
Y
STOP
KT1削除
Fake=F
S238
S233
S234
認証処理(AKE)
削除指示
S231
LCM
デバイスID
(LCMID)
E1
KM[PDID]
OK
S235
S236
チェックイン

【図１８】

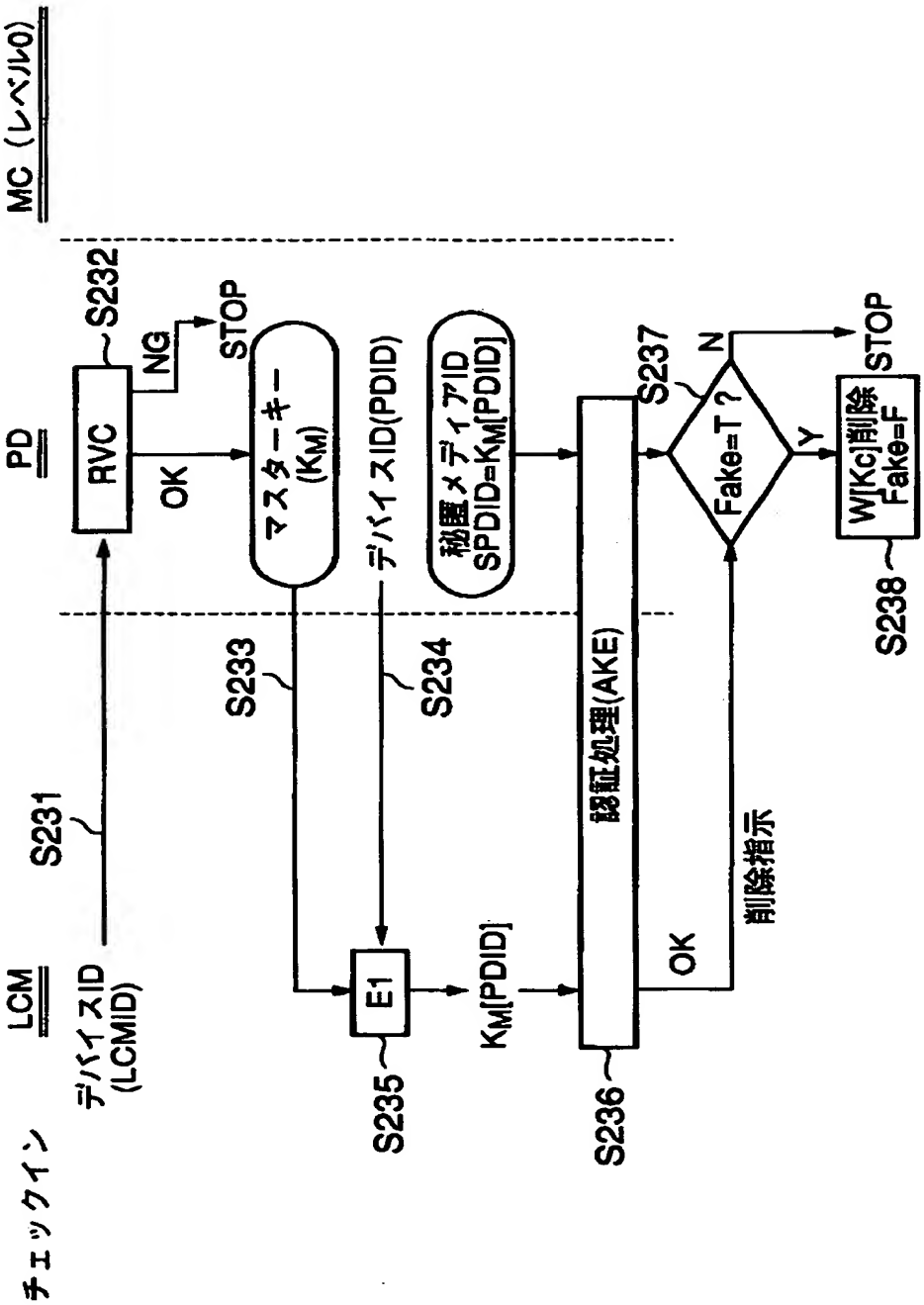

MC（レベル0）
PD
LCM
チェックアウト
デバイスID
(LCMID)
S201
RVC
S202
NG
STOP
OK
マスターキー
(KM)
S203
デバイスID(PDID)
S204
E1
S205
KM[PDID]
秘匿デバイスID
SPDID=KM[PDID]
S251
認証処理(AKE)
KT1
S253
KT1[W[Kc]]
E4
D5
S254
W[Kc]
E3
S252
(KM[PDID])[Kc]
=W
Kc
C
E0
S255
S256
Kc[C]

【図１９】

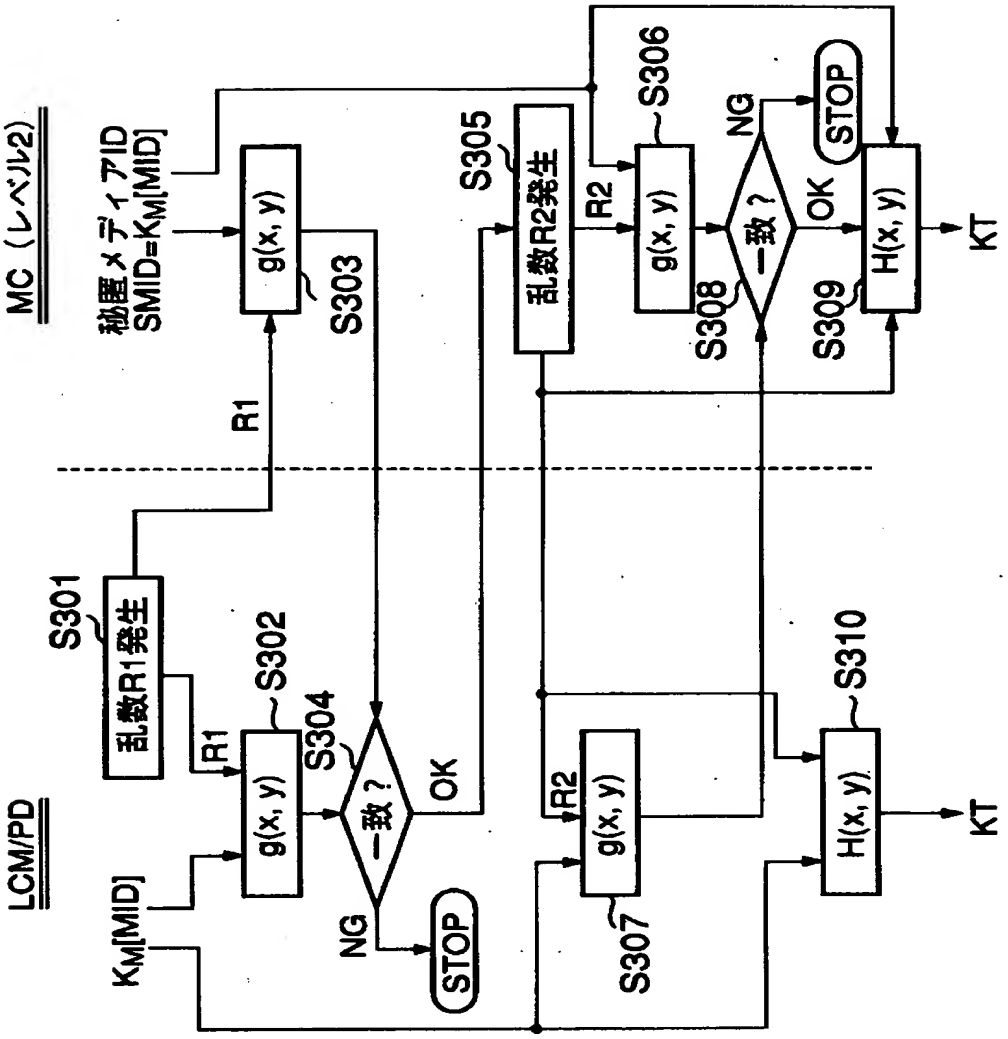
再生



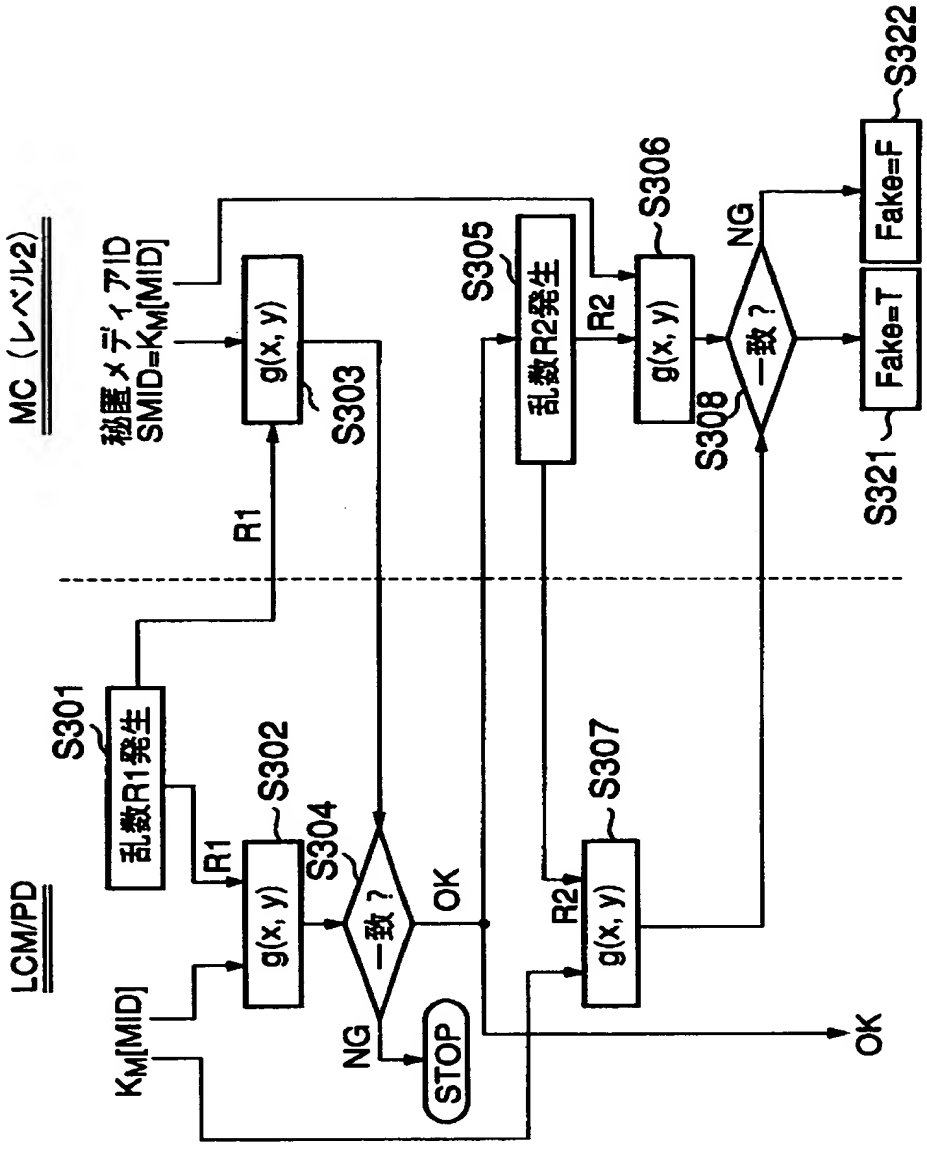
【図２０】


MC（レベル0）
PD
LCM
チェックイン
デバイスID
(LCMID)
S231
RVC
S232
NG
STOP
OK
マスターキー
(KM)
デバイスID(PDID)
秘匿メディアID
SPDID=KM[PDID]
S233
S234
E1
KM[PDID]
S235
認証処理(AKE)
S236
S237
Fake=T？
N
Y
OK
削除指示
W[Kc]削除
Fake=F
STOP
S238

【図２１】


MC（レベル2）
秘匿メディアID
SMID=K_M[MID]
g(x, y)
S303
R1
S301
乱数R1発生
S302
S304
一致？
OK
NG
STOP
LCM/PD
K_M[MID]
S305
乱数R2発生
R2
S306
S307
S308
S309
S310
H(x, y)
KT

【図２２】


MC（レベル2）
秘匿メディアID
SMID=KM[MID]
g(x, y)
S303
R1
S305
乱数R2発生
R2
S306
g(x, y)
NG
一致？
S308
Fake=F
S322
Fake=T
S321
S301
乱数R1発生
R1
S302
g(x, y)
S304
一致？
OK
NG
STOP
S307
R2
g(x, y)
OK
LCM/PD
KM[MID]

【書類名】　　要約書

【要約】

【課題】低コストな記録媒体を用いて、セキュリティ性の高い安全な相互認証が実現できる。

【解決手段】演算処理機能を有する記録媒体に複製コンテンツを記録する記録装置と該記録媒体との間の相互認証方法において、前記記録媒体は、少なくとも該記録媒体に依存する第１の情報と、前記記録装置と相互認証を行う際に該記録装置と共有すべき該記録媒体に依存する第２の情報とを記憶し、前記記録装置は、前記記録媒体から得られた前記第１の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第２の情報とを用いて前記記録装置と前記記録媒体との間で相互認証を行うことを特徴とする。

【選択図】　　図８

出願人履歴情報

識別番号　〔０００００３０７８〕

１．変更年月日　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
　〔変更理由〕　　新規登録
　　住　所　　大阪府門真市大字門真１００６番地
　　氏　名　　松下電器産業株式会社